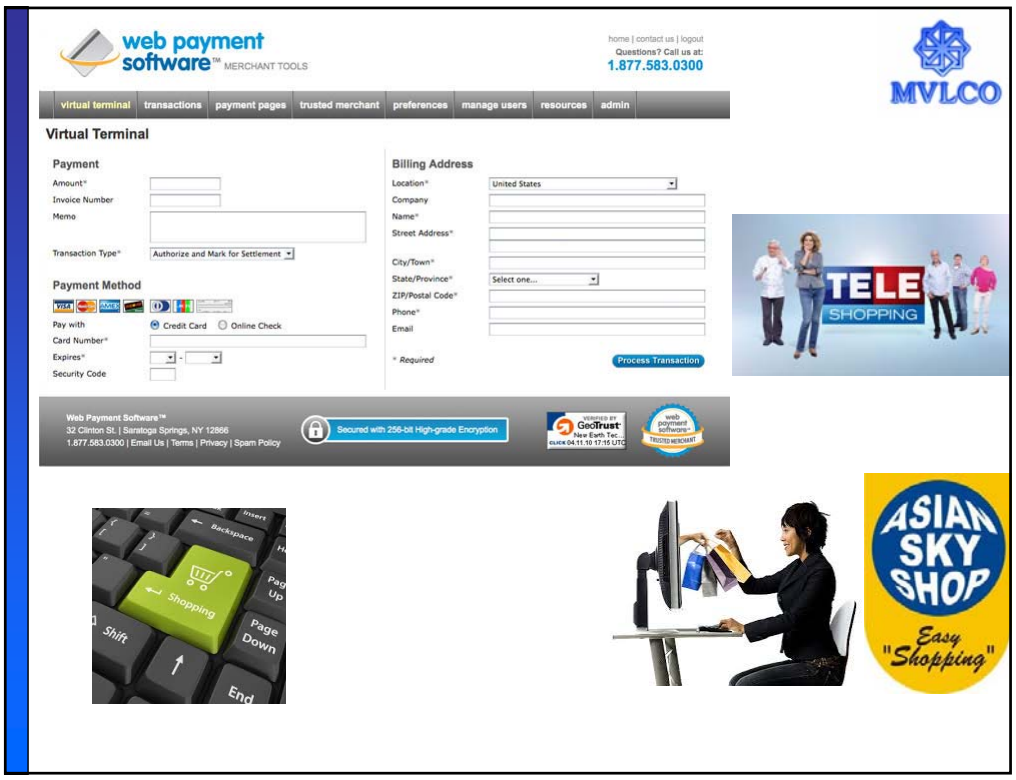
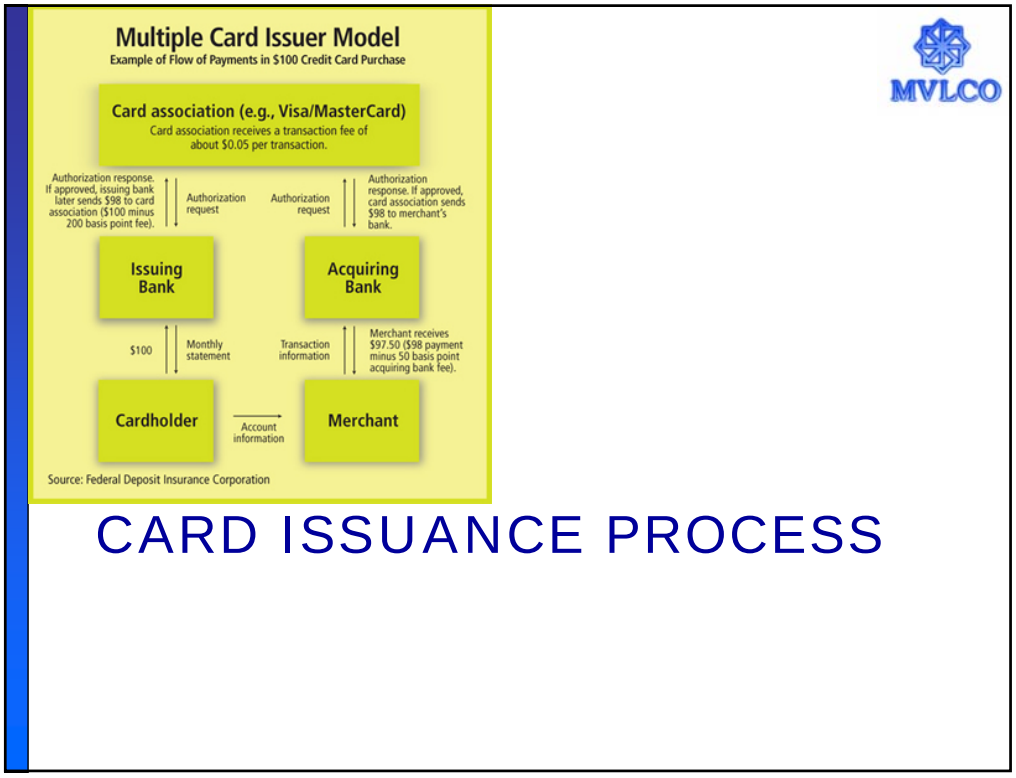




Issuance process in brief

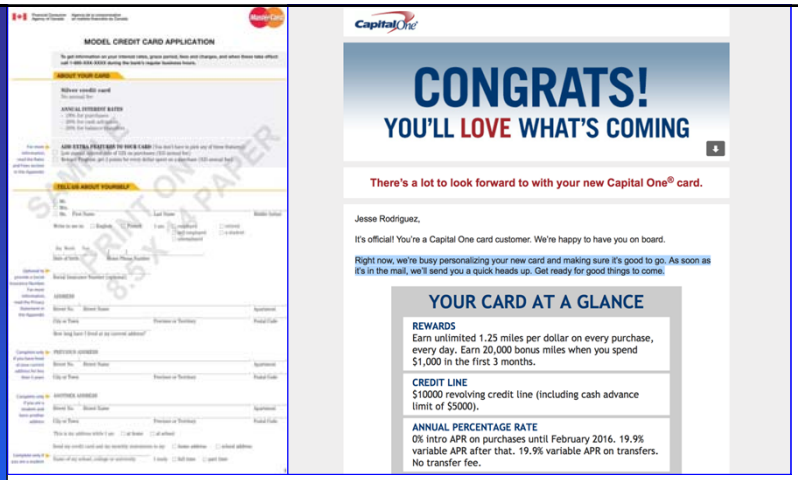
- Advertisement
- Application
- De-dupe – internal/external
- Document verification
- Customer contact program (CCP)
- Credit assessment (using financials, scores and results of CCP)
- Limit sanction and program/scheme attachment
- Card production
  - Tipping
  - Personalisation
- PIN generation
- Upload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

ADVERTISING

How to advertise

- A creditor shall not make any oral or written statement, in **advertising** or otherwise, to applicants or prospective applicants that would discourage on a **prohibited basis** a reasonable person from making or pursuing an application.
- Actually available terms and no misleading terms
- The “Schumer Box” disclosure in USA

Interest Rates and Interest Charges	
Annual Percentage Rate (APR) for Purchases 1	8.99%, 10.99%, or 12.99% introductory APR for one year, based on your creditworthiness. After that, your APR will be 14.99%. This APR will vary with the market based on the Prime Rate.
APR for Balance Transfers	15.99% This APR will vary with the market based on the Prime Rate. 2
APR for Cash Advances	21.99% This APR will vary with the market based on the Prime Rate. 3
Penalty APR and When it Applies 4	28.99% This APR may be applied to your account if you: 1) Make a late payment; 2) Go over your credit limit; 3) Make a payment that is returned; or 4) Do any of the above on another account that you have with us. How Long Will the Penalty APR Apply?: If your APRs are increased for any of these reasons, the Penalty APR will apply until you make six consecutive minimum payments when due.
How to Avoid Paying Interest on Purchases	Your due date is at least 25 days after the close of each billing cycle. We will not ch... you any interest on purchases if you pay your entire balance by the due date each... 5
Minimum Interest Charge 6	...ou are charged interest, the charge will be no less than $1.50.
For Credit Card Tips from the Federal Reserve Board	To learn more about factors to consider when applying for or using a credit card, visit the website of the Federal Reserve Board at http://www.federalreserve.gov/creditcard.



APPLICATION

Application details

- Regulation requires that a credit application can be judged only on the basis of financial responsibility.
- Creditworthiness, affordability and appropriateness requirements
- Advised sale and non-advised sale

Application details

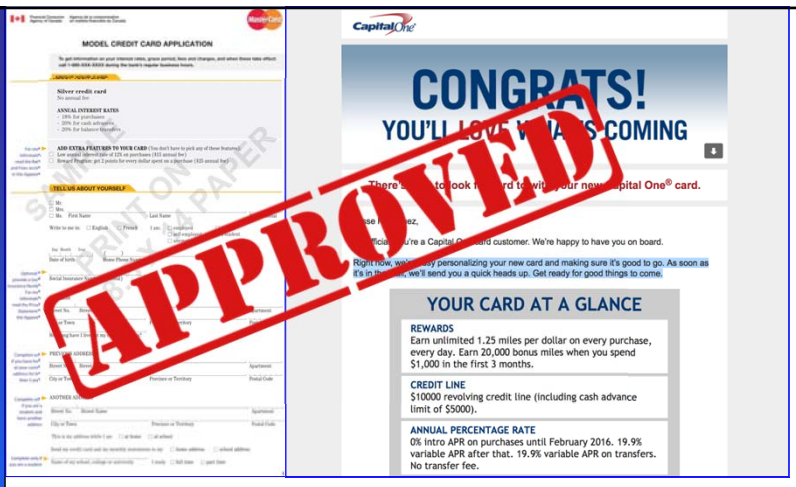
- Regulation requires that a credit application can be judged only on the basis of financial responsibility.
- What information should be sought in the application?

What information can be sought ?

- **Restrictions on information in the application:**
  - A creditor shall not inquire about the race, color, religion, national origin, or sex of an applicant or any other person.
  - Use of title on an application form (such as Ms., Miss, Mr., or Mrs.) is allowed but designation of a title is optional. Otherwise use only terms that are neutral as to sex.
  - May not request any information concerning the spouse or former spouse of an applicant except in certain cases.
  - Marital status (application for unsecured credit) unless the applicant resides in a community property state or is relying on property located in such a state for repayment.
  - a creditor may inquire about the applicant's marital status, but shall use only the terms married, unmarried, and separated.
  - Disclosure about income from alimony, child support, or separate maintenance can not be requested.
  - Childbearing, childrearing. Can not be requested except with certain exceptions
- Permanent residency and immigration status can be requested.

What information can be sought ?

Goa civil code

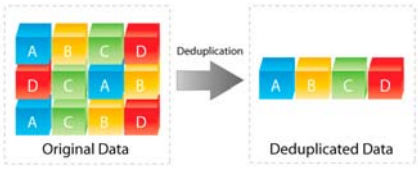


MVLCO

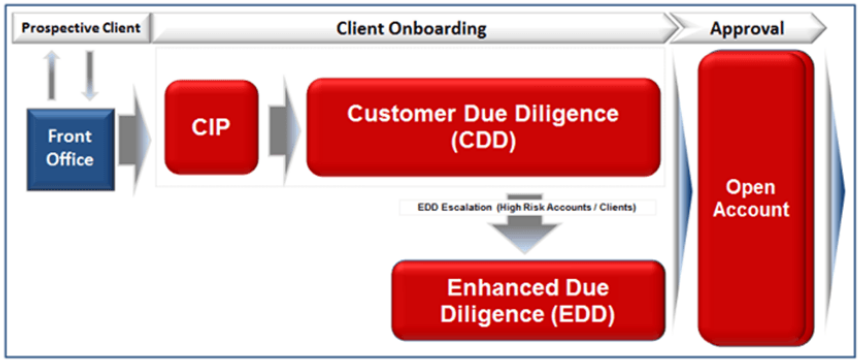
APPROVAL

KYC, De-dupe and Customer Contact Program

MVLCO



AML KYC Onboarding Process Flow (Generic Flow)



Approval of credit card

- Creditworthiness, affordability and appropriateness requirements
- Creditworthiness
  - Income
  - Age
  - Credit scores
    - Internal/external
    - Application scores/behavior scores

Notification of action taken

- An issuer is required to notify an applicant of action (approval or rejection or hold) taken on his/her credit card application within a stipulated time.:
  - after receiving a completed application
  - after receiving an incomplete application
- **The notification:**
  - Should be in writing and shall contain a statement of the action taken;
  - And provide a **statement of specific reasons** for the action taken

MVLCO

Experian

FICO® SCORE
The score lenders use.™

FURNISHING OF CREDIT INFORMATION

MVLCO

Furnishing of credit information

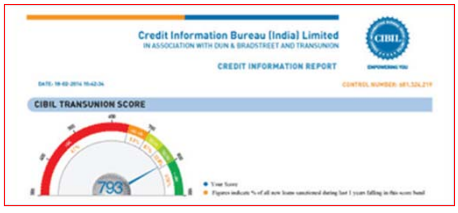
- Most of the issuers inform external credit scoring agencies about sanctioning credit limit and issuance of new card.

Callcredit
secure in the knowledge

CREDIT INFORMATION BUREAU (INDIA) LIMITED
CIBIL

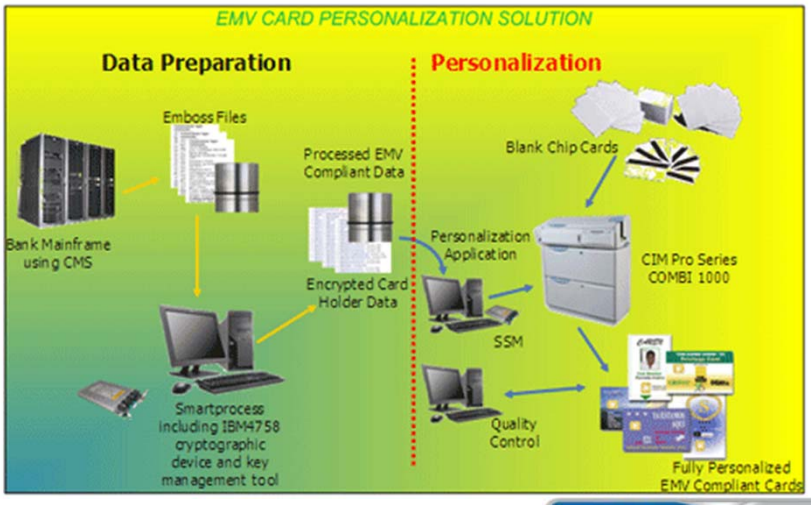
300-850 FICO® Score
The Score That Matters®

EQUIFAX®



MVLCO

MANUFACTURING A CARD



MVLCO

Certified International Payment Systems Professional (CIPSP)™

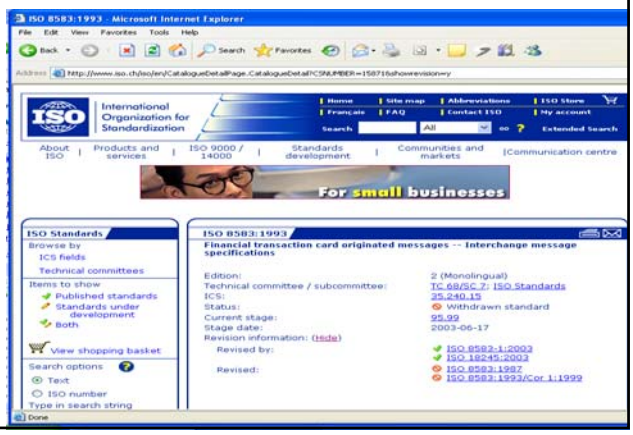
Module 4
ISO 8583 and ISO 20022 Messages

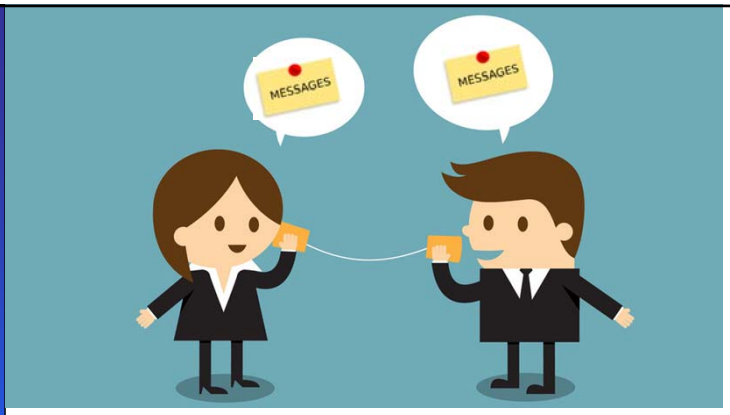
MVL Consulting Private Limited
www.mvlco.com

Module Objective

At the end of this module, you will understand:

1. *Different types of ISO 8583 messages*
2. *Different types of ISO 20022 messages*





MVLCO

COMMUNICATION AND MESSAGING

Communication

MVLCO

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 Standard

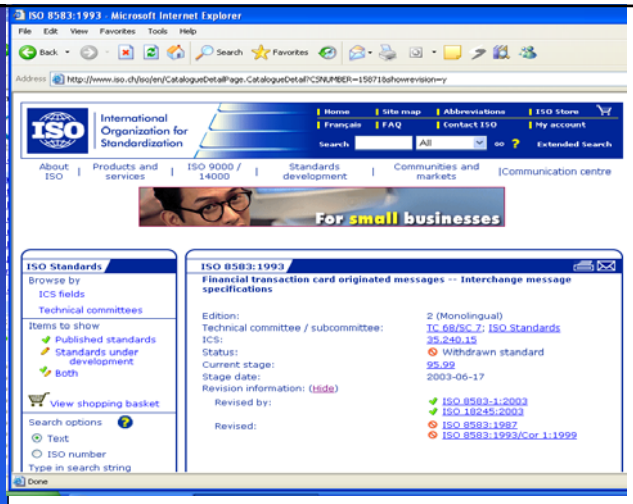
- ISO 8583 was initially created in 1987 and was revised in 1993 (corrected in 1999) and in 2003.
- Currently, 2003 version is operative.
- Changes have been incorporated mainly on account of advances in payment technologies and also to improve layout and readability.
- The standard consists of three parts:
  - Part 1 : messages, data elements and code values
  - Part 2 : Application and registration procedures for institution identification codes (IIC)
  - Part 3 : Maintenance procedures for messages, data elements and code values.

A brief about ISO 8583 message format

- ISO 8583 defines a message format and a communication flow so that different systems can exchange these transactions.
- Vast majority of card transactions made use ISO 8583 at some point in the communication chain, as do transactions made when a customer uses a card to make a payment in a store.
- In particular, both the MasterCard and Visa networks base their transactions on the ISO 8583 standard, as do many other institutions and networks.
- Some countries have developed their own standards on the foundation of ISO 8583.

THE UKCARDS ASSOCIATION

STANDARD 70 - BOOK 1
CARD ACCEPTOR TO ACQUIRER INTERFACE STANDARDS
Business Rules for Card Processing



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**

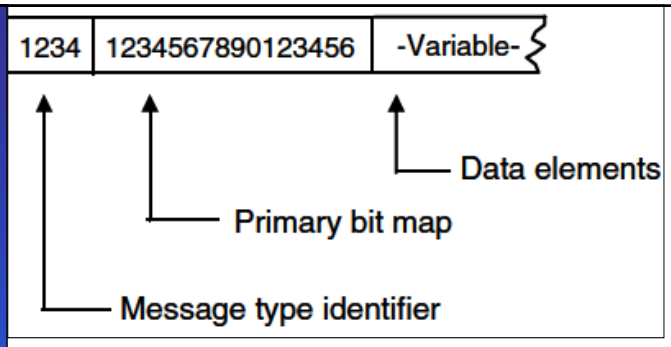
www.mvlco.com 115

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

CFO

www.mvlco.com 116

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		



MESSAGE STRUCTURE

Message type indicator (MTI)

- Message type indicator is composed of two elements
  - Version number
  - Message type identifier
- Message type identifier:
  - The message type identifier is a three digit numeric field identifying the message class, message function and transaction originator.

Code no.	International Standard no.	Year of publication	Other
0	ISO 8583	1987	—
1	ISO 8583	1993	—
2	ISO 8583	2003	—
3-7	—	—	Reserved for ISO use
8	—	—	Reserved for ISO use
9	—	—	Reserved for ISO use

Message bitmaps and data elements

- The MTI is followed by the bitmap which indicates which elements are present in the body of the message.
- The second message component is one or two message **bitmaps**, each consisting of 64 bits.
- Each bit signifies the presence (1) or absence (0) in the message of the **data element** associated with that particular bit.
- The **primary message bit map (bits 1-64)** is always present and the most frequently used data elements are indexed from these bit positions.
- Infrequently used data elements are indexed from the **secondary bit map position (bits 65-128)**

Data elements

- Messages are constructed using the **message bitmaps as an index of data elements** that are present.
- Fixed length and variable length data elements
- There are three types of data elements:
  - **Primitive data elements**
    - A data element which **has no further parts or sub-elements** e.g. “approval code” (Bit38)
  - **Constructed data elements**
    - A constructed data element **consists of a fixed number of sub-elements** all of which are present e.g. “Amounts original”
  - **Composite data elements**
    - Where contents **consists of a large number of sub-elements** and a transaction is likely to require data from only one or at the most a limited number of sub-elements.

Dataset and dataset identifier

- The sub-elements of composite data elements fall in natural categories viz. purchase card data, airline data etc.
- Generally, one transaction would need data from only one or at most limited number of these categories.
- **Datasets** are created to identify these categories.
- All the sub-elements that can be included in a particular composite data element are divided into a number of related datasets and each dataset is given a “**dataset identifier**”.

Industry	Dataset identifier
Free form description data	71
Invoice data, at header and line item detail level	72/73
Airline itinerary data	74/75
Auto rental/vehicle data	76
Lodging data	77
Fleet card data	78

www.mvlco.com 122

Dataset Identifiers and formatting

- Each dataset is given a one digit binary identifier, allowing up to 256 possible datasets per composite data element. The dataset identifier is the first component of the dataset. Dataset identifiers can have a value between 00 and FF (hexadecimal).
- a) The values of 00 and FF are reserved for ISO use.
- b) The values (01-70) shall only be used for the transmission of TLV sub-elements

Dataset identifier (01)	Dataset length	$T_1 L_1 V_1 T_2 L_2 V_2$ ....$T_n L_n V_n$	Dataset identifier (02)	Dataset length	$T_1 L_1 V_1 T_2 L_2 V_2$ .....$T_n L_n V_n$

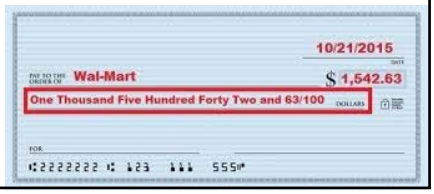
- c) The values (71-FE) shall only be used with dataset bit maps. If the dataset identifier is between 71 and FE, the third dataset component is a dataset bit map (DBM).
- The initial DBM has a length of 16 bits (2 bytes) and is designed to cope with most dataset requirements. Additional (continuation) DBMs may be added, and have a length of 8 bits (1 byte) each. These bit maps are chained together using the initial bit of each bit map.

Dataset identifier (71)	Dataset length	Dataset bit map	Sub-elements	Dataset identifier (72)	Dataset length	Dataset bit map	Sub-elements

www.mvlco.com 123

Expression of amounts

- **Decimal separator**
  - In ISO 8583 messages, the amount is expressed without a decimal separator.
  - Where a minor unit of currency applies, the relevant minor unit data element indicates the number of decimal places in the relevant amount.
- **Example:**
  - USD/840 Amount = 50000 = USD Five Hundred
  - JPY/392 Amount = 500 = JPY Five Hundred
- **Conversion rate data elements**
  - In conversion rate data elements, the leftmost digit denotes the number of positions the decimal separator is to be moved from the right.
- **Example:**
  - 91234567 = 0.001234567



ICC Data : DE 55 : ISO 8583 and ISO 7816-6

- If the data pertains to more than one application, the data for each application shall be grouped together and shall be wrapped by a constructed data object for the length of the data for that application.
- Tags may be in any order. Tags are application specific so that the same tag may appear in more than one application and have different meanings in each application. The constructed data objects may have the same or different tag values. It is up to the card issuer to determine how to process each application.

Length of DE55	TLV coded data objects in any order								
	T_1	L_1	V_1	T_2	L_2	V_2	T_3	L_3	v_3
0035	4F	10	AID	5A	0A	PAN	9A	03	Date

BER-TLV Encoding of EMV Tags

- ISO-8583 messages encode EMV tags using **BER-TLV scheme in Field 55** of the message. The formal name of the encoding scheme is **ASN.1 Basic Encoding Rule (ISO 8825).**
- ASN.1 is a formal language to describe data structures. It consists of primitive data objects (boolean, integer, UTF8 string) that can be constructed to define more complex data structures (Sequences, Sets).
- To encode ASN.1 instances in a computer readable form, TLV notation is used.
- Tags are divided into four classes.
  - The universal class contains basic data types like integer, boolean, etc.
  - The application class is used for data elements defined by an application specification or industry standard (e.g. EMV).
  - The context specific class is used for data elements that are unique within it's enclosing context (Like the concept of local variables in a programming language).
  - The private class is used for all privately defined data objects.

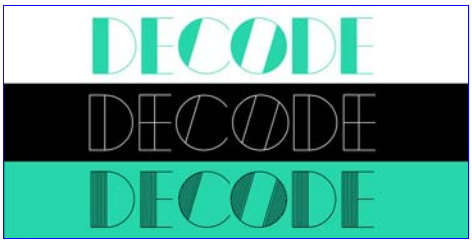
ICC Data : DE 55 : ISO 8583 and ISO 7816-6

- The *Integrated circuit card* (*ICC) related data* data element is a special form of a composite data element used to transmit ICC related data from the ICC to the card issuer and from the card issuer to the ICC.
- If the data is in accordance with ISO 7816-6, there is no requirement for a dataset identifier or dataset bit map as these functions are covered by the ISO 7816-6 TLV coding structures. The result is that the dataset identifier is replaced by the T element, the dataset length by the L element and the sub-elements by the V element.
- The ICC data may consist of either a constructed data object and/or a series of individual data objects as specified in ISO 7816-6.
- If the data is in accordance with ISO 7816-6 and pertains to a single application, the data may be wrapped in a constructed data object.
- Data structures not in accordance with ISO 7816-6 are subject to bilateral agreement.

Example of DE 55

TLV Data 0149

5F2A0201245F34010182021C008407A0000000031010950580000000009A031102249B0268009C01009F02060000000000009F03060000000000009F0607A00000000310109F0802008C9F0902008C9F100706010A039000009F1A0201249F2608423158936ED6C38F9F2701809F3303E0B0C89F34034103029F3501229F360200019F3704ACAC66E89F5800DF0100DF0200DF0400



Data Objects List (DOL)

- In several instances, the terminal is asked to build a flexible list of data elements to be passed to the card under the card's direction.
- To minimise processing within the ICC, such a list is not TLV encoded but is a single constructed field built by concatenating several data elements together.
- Since **the elements of the constructed field are not TLV encoded**, it is imperative that the ICC knows the format of this field when the data is received.
- **This is achieved by including a Data Object List (DOL)** in the ICC, specifying the format of the data to be included in the constructed field.

www.mvlco.com

Types of DOLs used in EMV

- DOLs currently used in EMV specification include:
  - the **Processing Options Data Object List (PDOL)** used with the GET PROCESSING OPTIONS command
  - the **Card Risk Management Data Object Lists (CDOL1 and CDOL2)** used with the GENERATE APPLICATION CRYPTOGRAM (AC) command
  - the **Transaction Certificate Data Object List (TDOL)** used to generate a TC Hash Value
  - the **Dynamic Data Authentication Data Object List (DDOL)** used with the INTERNAL AUTHENTICATE command

www.mvlco.com

MVLCO

MESSAGE CLASS DEFINITIONS

MVLCO

Message classes

- Authorisation messages (1)
- Verification messages (1)
- Financial presentment messages (2)
- Financial presentment accumulation messages (2)
- File action messages (3)
- Reversal messages (4)
- Charge back messages (4)
- Reconciliation messages (5)
- Administrative messages (6)
- Retrieval and retrieval fulfilment messages (6)
- Error messages (6)
- Fee collection messages (7)
- Network management messages (8)
- Key management messages (8)
- Batch transfer/file transfer messages

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		

Codes

- Institution identification codes (IIN)/Merchant category codes (MCC)
- Standard industrial classification (SIC)
- Data element condition codes (Table 25)
- Transaction type codes (Table A.22)
- Account type codes (Table A.23)
- Processing codes
  - Processing code is a constructed data element of three parts totalling 6 positions (1) Transaction Type Code 2an, (2) Account Type Code1 (from) 2an and (3) Account Type Code2 (to) 2an.
  - Transaction Type Code and Account Type Code together make Processing Code.
- Message reason codes (Table A.11)
- Function codes (Table A.9)
- Action codes (Table A.1)
- Error codes (Table A.10)

www.mvlco.com 134

Action code numbering scheme

The numbering scheme for action codes shall be based upon the type of action and has no direct correlation to the message type identifier. The action codes are grouped as follows:

a) 0xxx: authorization/financial presentment approved.

b) 1xxx: authorization/financial presentment denied.

c) 2xxx: authorization/financial presentment denied, pick up card.

d) 3xxx: file actions.

e) 4xxx: reversal or chargeback actions.

f) 5xxx: reconciliation actions.

g) 6xxx: administrative actions.

h) 7xxx: fee collection actions.

i) 8xxx: network management actions.

j) 9xxx: error/response actions.

The action code values are given in Clause A.1.

Bit 39 Action Code

AUTHORISATION MESSAGES

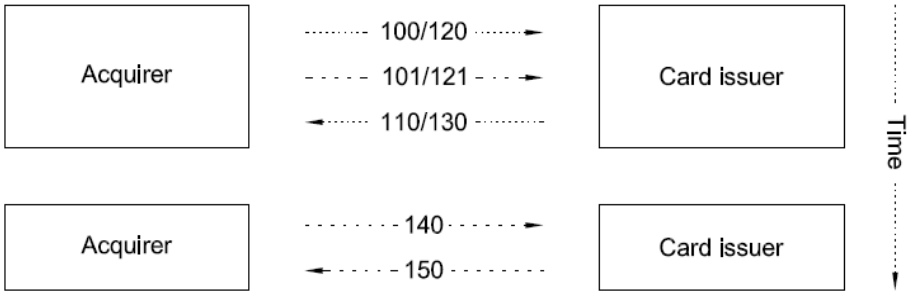
Authorisation Message classes

- **Authorisation:**
  - Authorisation is an approval or guarantee of funds given by the issuer to the acquirer. The amount of transaction can be accurate if the final amount is available, if not, it can be estimated.
- **Authorisation message class**
  - Original authorisation
  - Replacement authorisation
  - Resubmission authorisation
  - Supplementary authorisation
- **Authorisation decisions**
  - Full approval
  - Partial approval
  - Declined or rejected

Authorisation message types

MTI	Message	Purpose	From	To	Usage
100	Authorization request	Requests an authorization	Acquirer	Card issuer	
101	Authorization request repeat				
110	Authorization request response	Carries the answer to an authorization request message	Card issuer	Acquirer	Shall be sent in response to a 100 or a 101
120	Authorization advice	Advises of an authorization carried out on behalf of the card issuer	Acquirer	Card issuer	
121	Authorization advice repeat				
130	Authorization advice response	Carries the answer to an authorization advice message	Card issuer	Acquirer	Shall be sent in response to a 120 or a 121
140	Authorization notification	Notifies of an authorization action	Acquirer	Card issuer	
150	Authorization notification acknowledgement	Acknowledges receipt of one or more authorization notification messages	Card issuer	Acquirer	Shall be sent in response to a 140 if *Batch/file transfer message control* requests acknowledgement

Message flows



- MTI 100 Authorisation request
- MTI 120 Authorisation advice
- MTI 101 Authorisation request repeat
- MTI 121 Authorisation advice repeat
- MTI 110 Authorisation request response
- MTI 130 Authorisation advice response
- MTI 140 Authorisation notification
- MTI 150 Authorisation notification acknowledgement

FINANCIAL PRESENTMENT MESSAGES

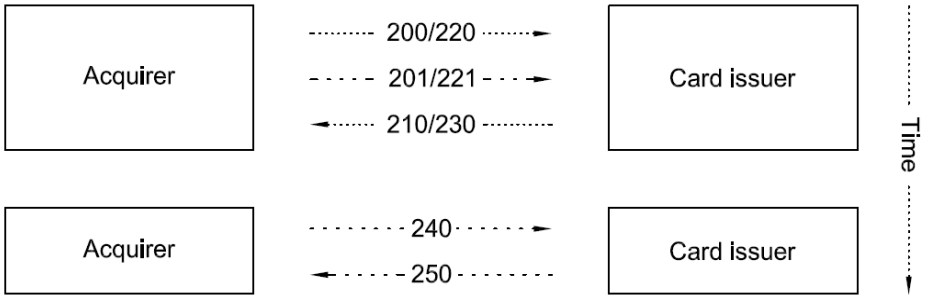
Financial presentment messages

- A financial presentment permits the application of the approved transaction amount to the cardholder's account for billing or posting.
- Types of financial presentment:
  - First, original or the only financial presentment
  - Previously authorised financial presentment
  - Resubmission of a previous financial presentment that was rejected or denied.
  - Representment i.e. recover funds partially/wholly charged back by the card issuer.
- **Financial presentment decisions**
  - Full approval
  - Partial approval
  - Declined or rejected

Financial presentment message types

MTI	Message	Purpose	From	To	Usage
200	Financial presentment request	Requests approval for a financial presentment transaction	Acquirer	Card issuer	
201	Financial presentment request repeat				
210	Financial presentment request response	Carries the answer to a financial presentment request message	Card issuer	Acquirer	Shall be sent in response to a 200 or a 201
220	Financial presentment advice	Advises of a financial presentment transaction carried out on behalf of the card issuer	Acquirer	Card issuer	
221	Financial presentment advice repeat				
230	Financial presentment advice response	Carries the answer to a financial presentment advice message	Card issuer	Acquirer	Shall be sent in response to a 220 or a 221
240	Financial presentment notification	Notifies of a financial presentment transaction carried out on behalf of the card issuer	Acquirer	Card issuer	
250	Financial presentment notification acknowledgement	Acknowledges receipt of one or more financial presentment notification messages	Card issuer	Acquirer	Shall be sent in response to a 240 if *Batch/file transfer message control* requested acknowledgement

Message flows



- MTI 200 Financial presentment request
- MTI 220 Financial presentment advice
- MTI 201 Financial presentment request repeat
- MTI 221 Financial presentment advice repeat
- MTI 210 Financial presentment request response
- MTI 230 Financial presentment advice response
- MTI 240 Financial presentment notification
- MTI 250 Financial presentment notification acknowledgement

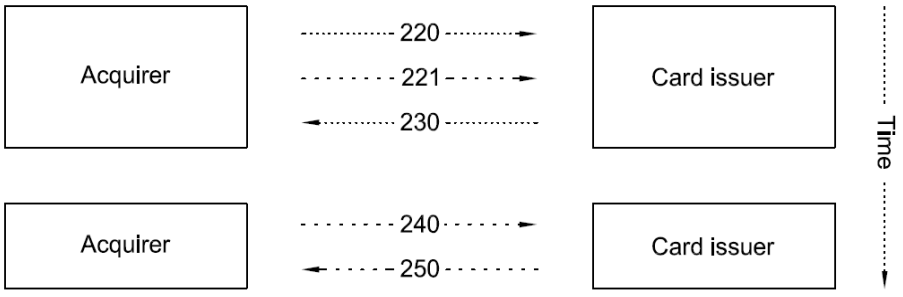
Financial accumulation presentment messages

- A financial accumulation presentment permits the application of the approved transaction amount to a specific account for billing or posting.
- **Types of financial accumulation presentments**
  - **Aggregation** i.e. when the accumulation has been done at a terminal under specific agreement between parties. It is not possible to recover the original detailed information.
  - **Card issuer back up totals** i.e. when accumulation is done at a terminal as a back up for transaction details as an alternative to detail collection when the details are lost.
  - **Truncation** i.e. when the accumulation has been done somewhere during the process and it is possible to recover all the detailed information.
- The function code is used to indicate the type of financial accumulation presentment.

Financial accumulation presentment message types

MTI	Message	Purpose	From	To	Usage
220	Financial presentment advice	Advises of a financial accumulation presentment carried out on behalf of the card issuer	Acquirer	Card issuer	
221	Financial presentment advice repeat				
230	Financial presentment advice response	Carries the answer to a financial presentment advice message	Card issuer	Acquirer	Shall be sent in response to a 220 or a 221
240	Financial presentment notification	Notifies of a financial accumulation presentment carried out on behalf of the card issuer	Acquirer	Card issuer	
250	Financial presentment notification acknowledgement	Acknowledges receipt of one or more financial presentment notification messages	Card issuer	Acquirer	Shall be sent in response to a 240 if *Batch/file transfer message control* requested acknowledgement

Message flows



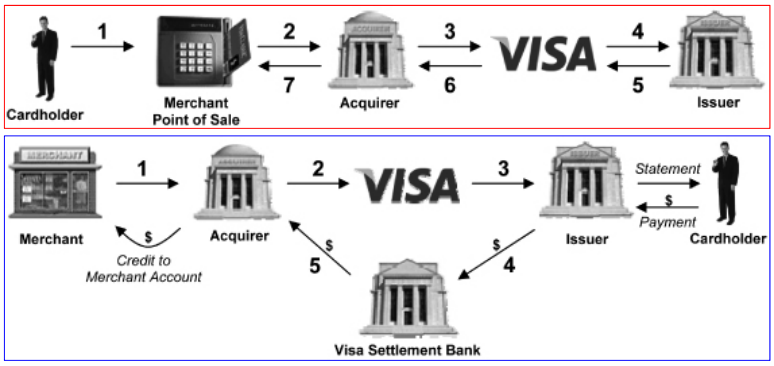
- MTI 220 Financial presentment advice
- MTI 221 Financial presentment advice repeat
- MTI 230 Financial presentment advice response
- MTI 240 Financial presentment notification
- MTI 250 Financial presentment notification acknowledgement

MTI : 2210
0166072780107220938010000000000000050000050580
7005113201602270707262016022720006800058166072
78010722093806265400000022

SINGLE MESSAGE SYSTEM VS. DUAL MESSAGE SYSTEM

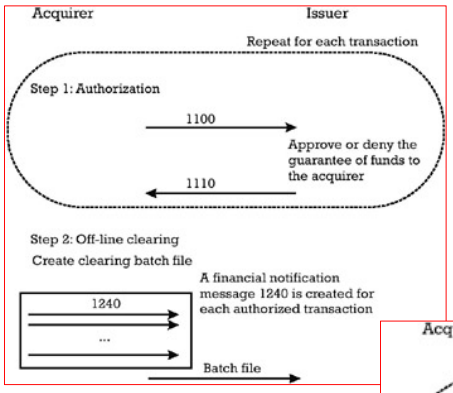
Single message v/s dual message transaction processing

- Message – Clearing and Settlement
- Authorisation and Clearing
  - Online Authorisation – Offline Clearing
  - Online Authorisation – Online Clearing

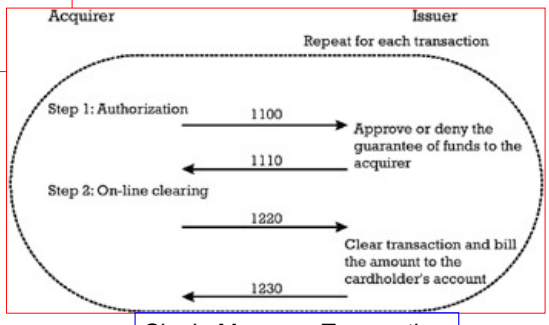


Dual Message v/s Single Message transaction processing

- In a **dual-message transaction**, the acquirer submits an electronic message at the time of purchase containing the information required for an authorization decision and a second message at a later point in time containing additional data required for clearing and settlement
- In a **single-message transaction**, the acquirer submits a single electronic message containing all data required for the authorization, clearing and settlement of the transaction. Actual financial settlement occurs at a later time.



Dual Message Transaction



Single Message Transaction

Clearing of Dual Message Transactions

- The dual-message protocol is used for credit card and signature-authenticated debit card transactions. Dual-message transactions traditionally require a physical or virtual signature.
- This category includes credit card transactions (with the exception of ATM cash advances) and signature authenticated debit transactions.
  - When a merchant's credit card system receives an authorization message, it creates a record of that authorization through a function known as "electronic draft capture" (EDC) (Also known as Electronic Ticket Capture).
  - These electronic drafts are stored in a "batch" until the merchant conducts "batch processing." This typically occurs at least once a day. High-volume merchants may conduct batch processing multiple times in a day; very low-volume merchants may conduct batch processing on less than a daily basis.
  - Whatever the frequency, merchants submit their authorized transactions to their acquirer in batch mode, not as individual transactions.

Clearing of Single Message Transactions

- With single messaging, authorization and clearing are done in one dispatch, and all the information necessary to post the transaction to the cardholder's account is communicated at the time of each transaction. There is no need to batch a set of transactions and enter them into clearing; only monetary settlement is required.
- Single-message transactions have only one cutoff time each day. At the cutoff time, the network calculates the total monetary positions for all its client banks for the day's single-message transactions.
- **There is only one settlement window, which is used for both dual-message and single-message transactions. When settlement is done on an aggregate net basis.**

MVLCO

Authorization Only

```
{0100}2[400555000000****]3[003000]4[000000000100]7[0623010426]11[1617]
14[0806]42[1234567890]59[050"CREDIT CARD AUTHORIZATION ONLY
  "]123[260101664040101]
```

CVV2 AUTHORIZATION ONLY

```
{0200}2[400555000000****]3[003000]4[000000000100]7[0623010426]11[1617]
14[1007]42[1234567890] 59[050"CREDIT CARD CVV2 AUTHORIZATION ONLY
   "]62.8[10233]123[260101664040101]
```

Generic Purchase

```
{0200}2[400555000000****]3[003000]4[000000000100]7[0623010426]11[1617]
14[1206]42[1234567890] 59[050"CREDIT CARD PURCHASE
   "]123[260101664040101]
```

Purchase with Cash Back

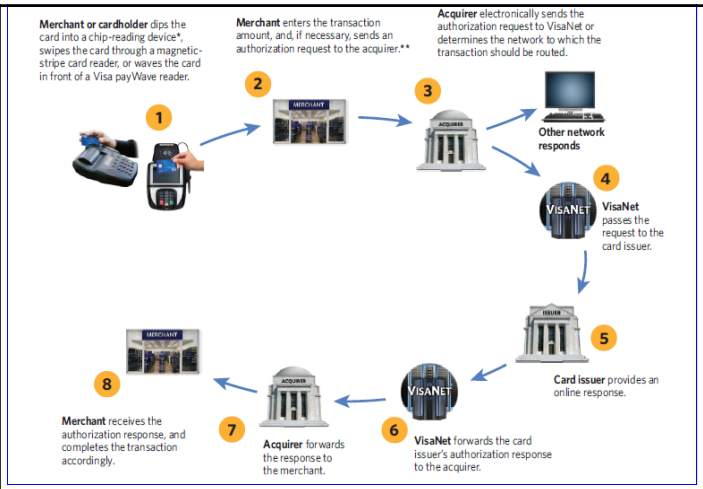
```
{0200}3[090000]4[000000000100]7[0622175500]11[900000]35[30400555000000
****=001210110000?]42[7022223318]52[8BYTEPIN]53[DUKPTKSN_BINARY_FIXED_
LENGTH_FORTY_BYTE_PIN_DATA]54[0005840D000000000100]59[050"PIN-Based
Debit Test PURCHASE w/CASH BACK       "]123[210101214118101]
```

MVLCO

Transaction messaging examples

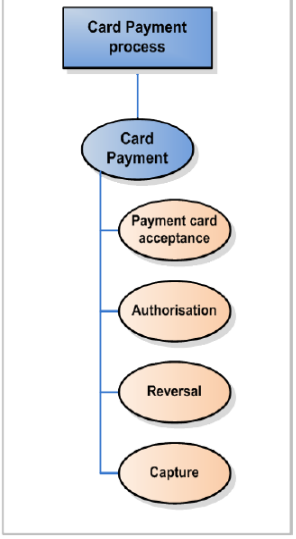
Switch and device logs

- ATM Rejects
- ATM Reversals
- ATM Suspects
- POS Rejects



ISO20022 MESSAGES FOR CARDS

Business process covered



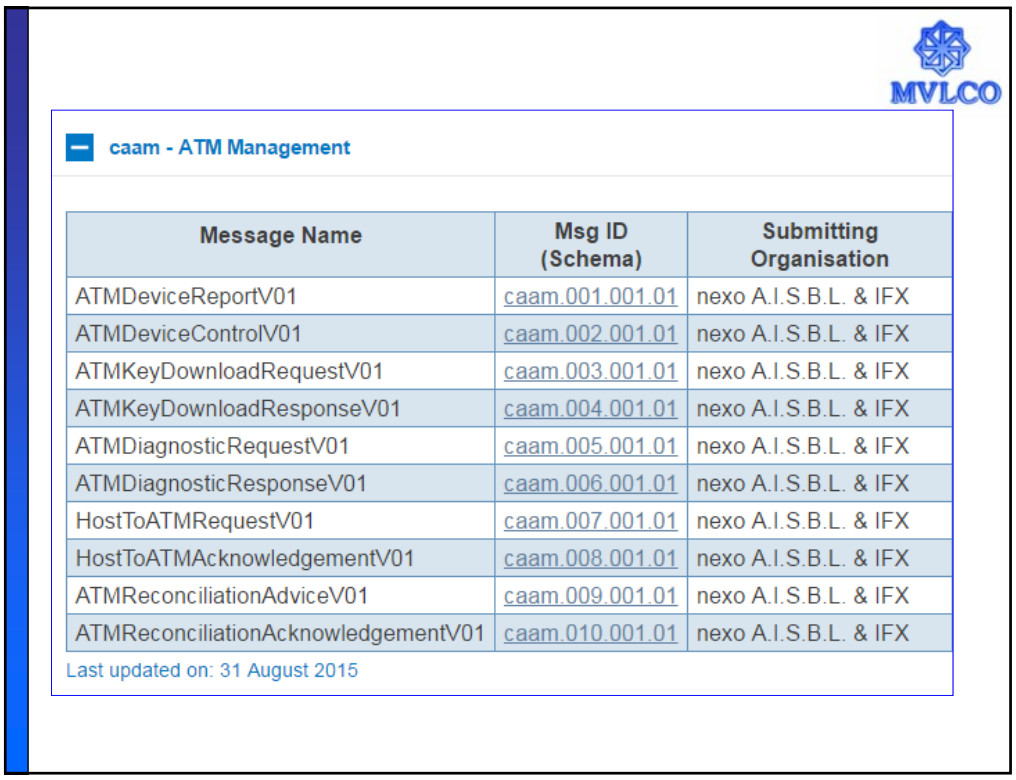
- **The process of performing a payment of good or services with a card:**
  - The process starts with the acceptance of the payment card, involves the authorisation of the payment transaction, and the transfer of financial information (capture) from the acceptor to the acquirer.
  - It also includes error situations, where it is necessary to reverse the authorisation.

ISO 20022
Universal financial industry message scheme

cain - Acquirer to Issuer Card Transactions

Message Name	Msg ID (Schema)	Submitting Organisation
AcquirerAuthorisationInitiationV01	cain.001.001.01	ISO TC68/SC7/TG1
AcquirerAuthorisationResponseV01	cain.002.001.01	ISO TC68/SC7/TG1
AcquirerFinancialInitiationV01	cain.003.001.01	ISO TC68/SC7/TG1
AcquirerFinancialResponseV01	cain.004.001.01	ISO TC68/SC7/TG1
AcquirerReversalInitiationV01	cain.005.001.01	ISO TC68/SC7/TG1
AcquirerReversalResponseV01	cain.006.001.01	ISO TC68/SC7/TG1
ReconciliationInitiationV01	cain.007.001.01	ISO TC68/SC7/TG1
ReconciliationResponseV01	cain.008.001.01	ISO TC68/SC7/TG1
NetworkManagementInitiationV01	cain.009.001.01	ISO TC68/SC7/TG1
NetworkManagementResponseV01	cain.010.001.01	ISO TC68/SC7/TG1
KeyExchangeInitiationV01	cain.011.001.01	ISO TC68/SC7/TG1
KeyExchangeResponseV01	cain.012.001.01	ISO TC68/SC7/TG1
AcquirerRejectionV01	cain.013.001.01	ISO TC68/SC7/TG1

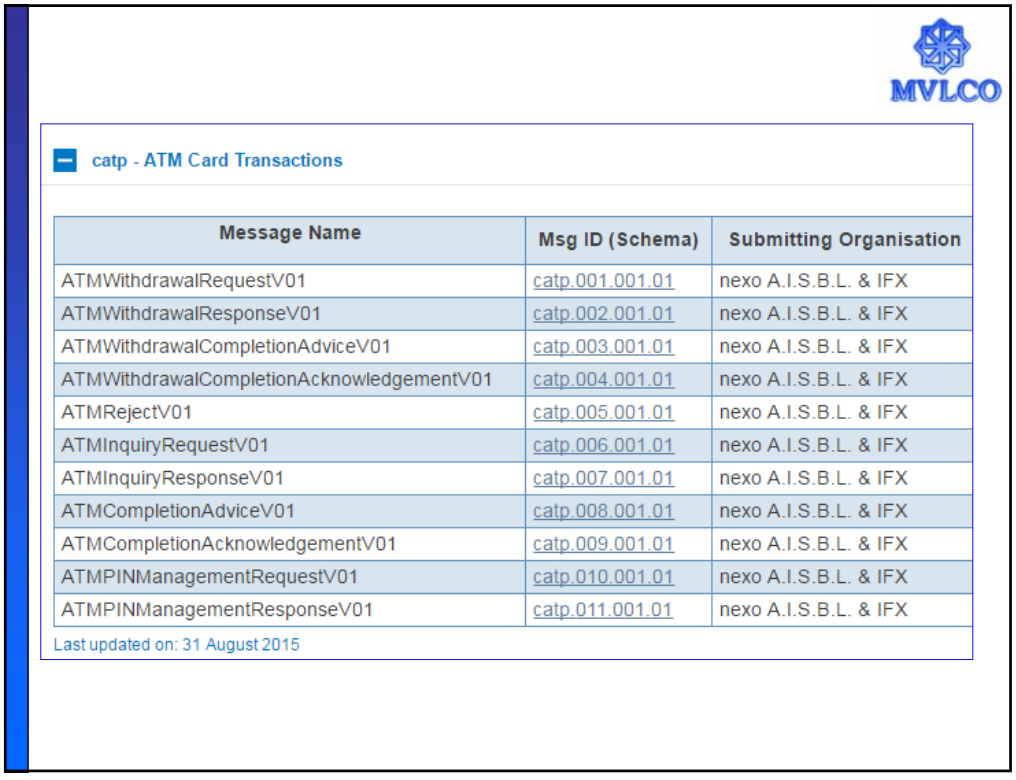
Last updated on: 3 February 2016



caam - ATM Management

Message Name	Msg ID (Schema)	Submitting Organisation
ATMDeviceReportV01	caam.001.001.01	nexo A.I.S.B.L. & IFX
ATMDeviceControlV01	caam.002.001.01	nexo A.I.S.B.L. & IFX
ATMKeyDownloadRequestV01	caam.003.001.01	nexo A.I.S.B.L. & IFX
ATMKeyDownloadResponseV01	caam.004.001.01	nexo A.I.S.B.L. & IFX
ATMDiagnosticRequestV01	caam.005.001.01	nexo A.I.S.B.L. & IFX
ATMDiagnosticResponseV01	caam.006.001.01	nexo A.I.S.B.L. & IFX
HostToATMRequestV01	caam.007.001.01	nexo A.I.S.B.L. & IFX
HostToATMAcknowledgementV01	caam.008.001.01	nexo A.I.S.B.L. & IFX
ATMReconciliationAdviceV01	caam.009.001.01	nexo A.I.S.B.L. & IFX
ATMReconciliationAcknowledgementV01	caam.010.001.01	nexo A.I.S.B.L. & IFX

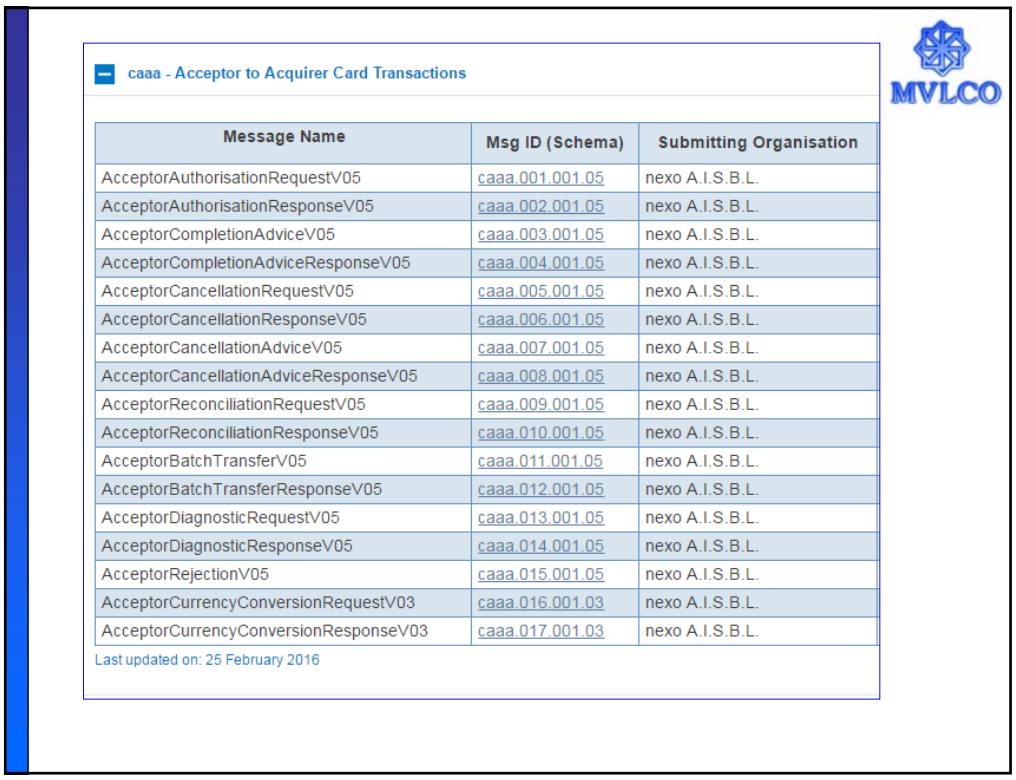
Last updated on: 31 August 2015



catp - ATM Card Transactions

Message Name	Msg ID (Schema)	Submitting Organisation
ATMWithdrawalRequestV01	catp.001.001.01	nexo A.I.S.B.L. & IFX
ATMWithdrawalResponseV01	catp.002.001.01	nexo A.I.S.B.L. & IFX
ATMWithdrawalCompletionAdviceV01	catp.003.001.01	nexo A.I.S.B.L. & IFX
ATMWithdrawalCompletionAcknowledgementV01	catp.004.001.01	nexo A.I.S.B.L. & IFX
ATMRejectV01	catp.005.001.01	nexo A.I.S.B.L. & IFX
ATMInquiryRequestV01	catp.006.001.01	nexo A.I.S.B.L. & IFX
ATMInquiryResponseV01	catp.007.001.01	nexo A.I.S.B.L. & IFX
ATMCompletionAdviceV01	catp.008.001.01	nexo A.I.S.B.L. & IFX
ATMCompletionAcknowledgementV01	catp.009.001.01	nexo A.I.S.B.L. & IFX
ATMPINManagementRequestV01	catp.010.001.01	nexo A.I.S.B.L. & IFX
ATMPINManagementResponseV01	catp.011.001.01	nexo A.I.S.B.L. & IFX

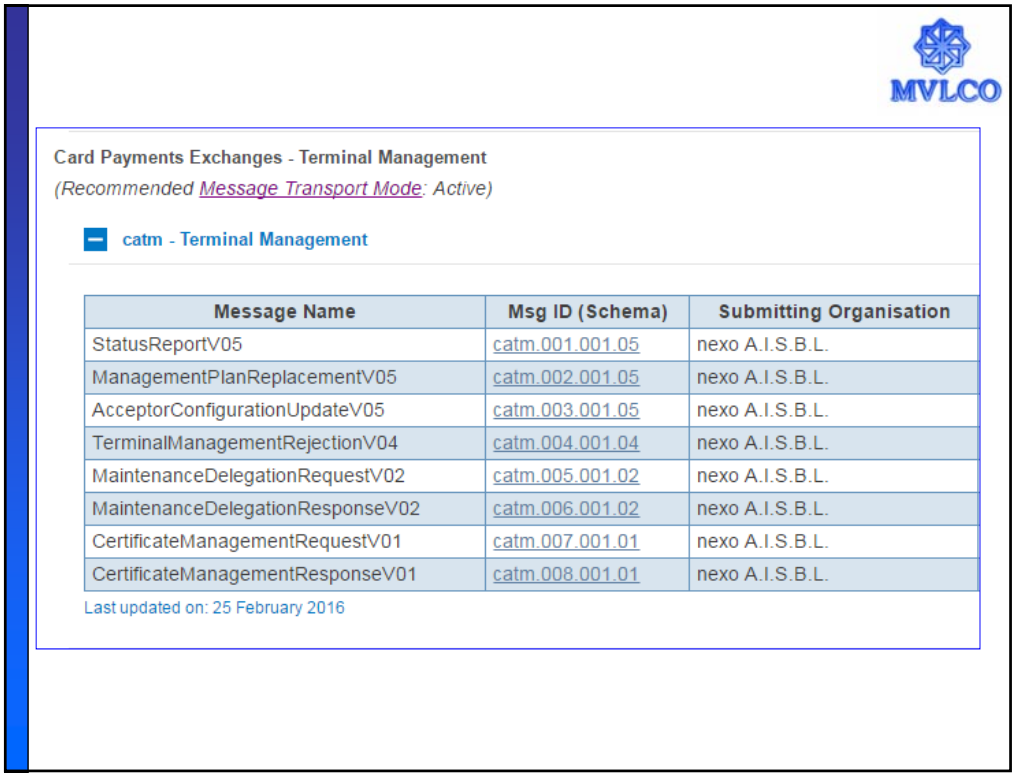
Last updated on: 31 August 2015



caaa - Acceptor to Acquirer Card Transactions

Message Name	Msg ID (Schema)	Submitting Organisation
AcceptorAuthorisationRequestV05	caaa.001.001.05	nexo A.I.S.B.L.
AcceptorAuthorisationResponseV05	caaa.002.001.05	nexo A.I.S.B.L.
AcceptorCompletionAdviceV05	caaa.003.001.05	nexo A.I.S.B.L.
AcceptorCompletionAdviceResponseV05	caaa.004.001.05	nexo A.I.S.B.L.
AcceptorCancellationRequestV05	caaa.005.001.05	nexo A.I.S.B.L.
AcceptorCancellationResponseV05	caaa.006.001.05	nexo A.I.S.B.L.
AcceptorCancellationAdviceV05	caaa.007.001.05	nexo A.I.S.B.L.
AcceptorCancellationAdviceResponseV05	caaa.008.001.05	nexo A.I.S.B.L.
AcceptorReconciliationRequestV05	caaa.009.001.05	nexo A.I.S.B.L.
AcceptorReconciliationResponseV05	caaa.010.001.05	nexo A.I.S.B.L.
AcceptorBatchTransferV05	caaa.011.001.05	nexo A.I.S.B.L.
AcceptorBatchTransferResponseV05	caaa.012.001.05	nexo A.I.S.B.L.
AcceptorDiagnosticRequestV05	caaa.013.001.05	nexo A.I.S.B.L.
AcceptorDiagnosticResponseV05	caaa.014.001.05	nexo A.I.S.B.L.
AcceptorRejectionV05	caaa.015.001.05	nexo A.I.S.B.L.
AcceptorCurrencyConversionRequestV03	caaa.016.001.03	nexo A.I.S.B.L.
AcceptorCurrencyConversionResponseV03	caaa.017.001.03	nexo A.I.S.B.L.

Last updated on: 25 February 2016



Card Payments Exchanges - Terminal Management

(Recommended Message Transport Mode: Active)

catm - Terminal Management

Message Name	Msg ID (Schema)	Submitting Organisation
StatusReportV05	catm.001.001.05	nexo A.I.S.B.L.
ManagementPlanReplacementV05	catm.002.001.05	nexo A.I.S.B.L.
AcceptorConfigurationUpdateV05	catm.003.001.05	nexo A.I.S.B.L.
TerminalManagementRejectionV04	catm.004.001.04	nexo A.I.S.B.L.
MaintenanceDelegationRequestV02	catm.005.001.02	nexo A.I.S.B.L.
MaintenanceDelegationResponseV02	catm.006.001.02	nexo A.I.S.B.L.
CertificateManagementRequestV01	catm.007.001.01	nexo A.I.S.B.L.
CertificateManagementResponseV01	catm.008.001.01	nexo A.I.S.B.L.

Last updated on: 25 February 2016

Certified International Payment Systems Professional (CIPSP)™

Module 5
Transaction Processing

MVL Consulting Private Limited
www.mvlco.com

Module Objective

At the end of this module, you will understand:

1. *End to end processing of card payment transaction*

RECALLING TRANSACTIONS PROCESSING

On us transaction

Switch

Back Office Host

HSM

Database

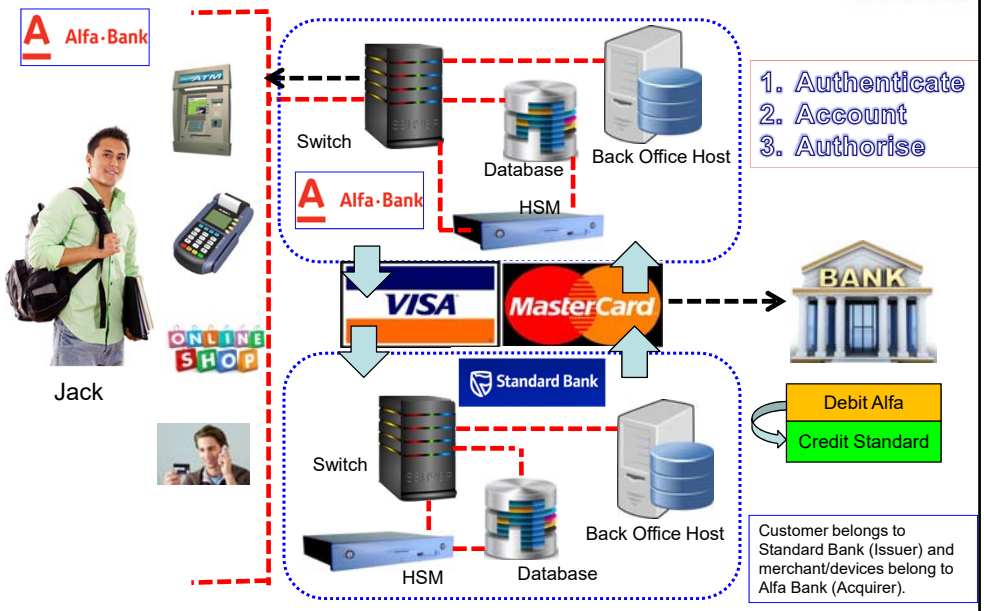
Jack

Standard Bank

1. Authenticate
2. Account
3. Authorise

Customer and merchant/devices belong to the same bank.

Off us transaction



Fully compliant with EMV standards

For security and interoperability with EMV terminals

EMV STANDARDS

www.mvlco.com 168

EMV standards

- EMV Standards were started by a working group created in 1993 by Europay International (EPI), MasterCard International (MCI) and VISA International (VISA). Europay International SA was absorbed into Mastercard in 2002. JCB (formerly Japan Credit Bureau) joined the organisation in December 2004.
- The group's objective is to define a common set of standards (EMV standards) for smart card based payment applications. These standards allow the card and the acceptance device to work seamlessly and securely together.
- EMV achieves interoperability between cards and devices through two key mechanisms. First, it defines the minimum requirements that chip cards and card acceptance devices must meet to communicate with one another. These requirements also ensure that the device does not damage the card. This initial set of procedures is called the EMV **Level 1** requirements.
- Second, EMV specifies how debit and credit transactions are to be executed once the basic physical contact between the chip and the device is established. This set of rules is called the EMV **Level 2** requirements.
- **Level 3** included software applications.

EMV implementations

- The most widely known chip card implementations of the EMV standard are
  - VIS – Visa
  - Mastercard chip – Mastercard
  - AEIPS – American Express
  - UICS - China Union Pay
  - J Smart – JCB
  - D-PAS – Discover/Diners Club International.
- Visa and MasterCard have also developed standards for using EMV cards in devices to support card not present transactions over the telephone and Internet.
  - MasterCard has the Chip Authentication Program (CAP) for secure e-commerce. Its implementation is known as EMV-CAP and supports a number of modes.
  - Visa has the Dynamic Passcode Authentication (DPA) scheme, which is their implementation of CAP using different default values.

Command APDU						
Header (required)				Body (optional)		
CLA	INS	P1	P2	Lc	Data Field	Le

Response APDU		
Body (optional)	Trailer (required)	
Data Field	SW1	SW2

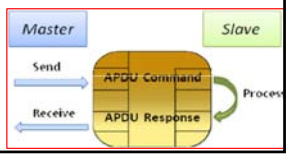
COMMANDS

THE TWELVE COMMANDMENTS

www.mvlco.com 171

Application Protocol Command Response APDU Pair (1)

- **APPLICATION BLOCK (post-issuance command)**
  - The APPLICATION BLOCK command is a post-issuance command that invalidates the currently selected application.
- **APPLICATION UNBLOCK (post-issuance command)**
  - The APPLICATION UNBLOCK command is a post-issuance command that rehabilitates the currently selected application.
  - Following the successful completion of an APPLICATION UNBLOCK command, the restrictions imposed by the APPLICATION BLOCK command are removed.
- **CARD BLOCK (post-issuance command)**
  - The CARD BLOCK command is a post-issuance command that permanently disables all applications in the ICC.
- **EXTERNAL AUTHENTICATE**
  - The EXTERNAL AUTHENTICATE command asks the application in the ICC to verify a cryptogram.
  - The ICC returns the processing state of the command.



www.mvlco.com

Application Protocol Command Response APDU Pair (2)

- **GENERATE APPLICATION CRYPTOGRAM**
  - The GENERATE AC command sends transaction-related data to the ICC, which computes and returns a cryptogram.
  - This command is also used when performing the Combined DDA/Application Cryptogram Generation (CDA) function
- **GET CHALLENGE**
  - The GET CHALLENGE command is used to obtain an unpredictable number from the ICC for use in a security-related procedure.
  - The challenge shall be valid only for the next issued command.
- **GET DATA**
  - The GET DATA command is used to retrieve a primitive data object not encapsulated in a record within the current application.
  - The usage of the GET DATA command in this specification is limited to the retrieval of the following primitive data objects:
    - ATC (tag '9F36')
    - Last Online ATC Register (tag '9F13')
    - PIN Try Counter (tag '9F17')
    - Log Format (tag '9F4F')

Application Protocol Command Response APDU Pair (3)

- **GET PROCESSING OPTIONS**
  - The GET PROCESSING OPTIONS command initiates the transaction within the ICC.
  - The ICC returns the Application Interchange Profile (AIP) and the Application File Locator (AFL).
- **INTERNAL AUTHENTICATE**
  - The INTERNAL AUTHENTICATE command initiates the computation of the Signed Dynamic Application Data by the card using:
    - the challenge data sent from the terminal and
    - ICC data and
    - a relevant private key stored in the card.
  - The ICC returns the Signed Dynamic Application Data to the terminal.
- **PIN CHANGE/UNBLOCK (post-issuance command)**
  - Its purpose is to provide the issuer the capability either to unblock the PIN or to simultaneously change and unblock the reference PIN.

Application Protocol Command Response : APDU Pair (4)

- **READ RECORD**
  - The READ RECORD command reads a file record in a linear file.
  - The response from the ICC consists of returning the record.
- **VERIFY**
  - The VERIFY command initiates in the ICC the comparison of the Transaction PIN Data sent in the data field of the command with the reference PIN data associated with the application. The manner in which the comparison is performed is proprietary to the application in the ICC.
  - The VERIFY command applies when the Cardholder Verification Method (CVM) chosen from the CVM List is an offline PIN

TRANSACTION PROCESSING

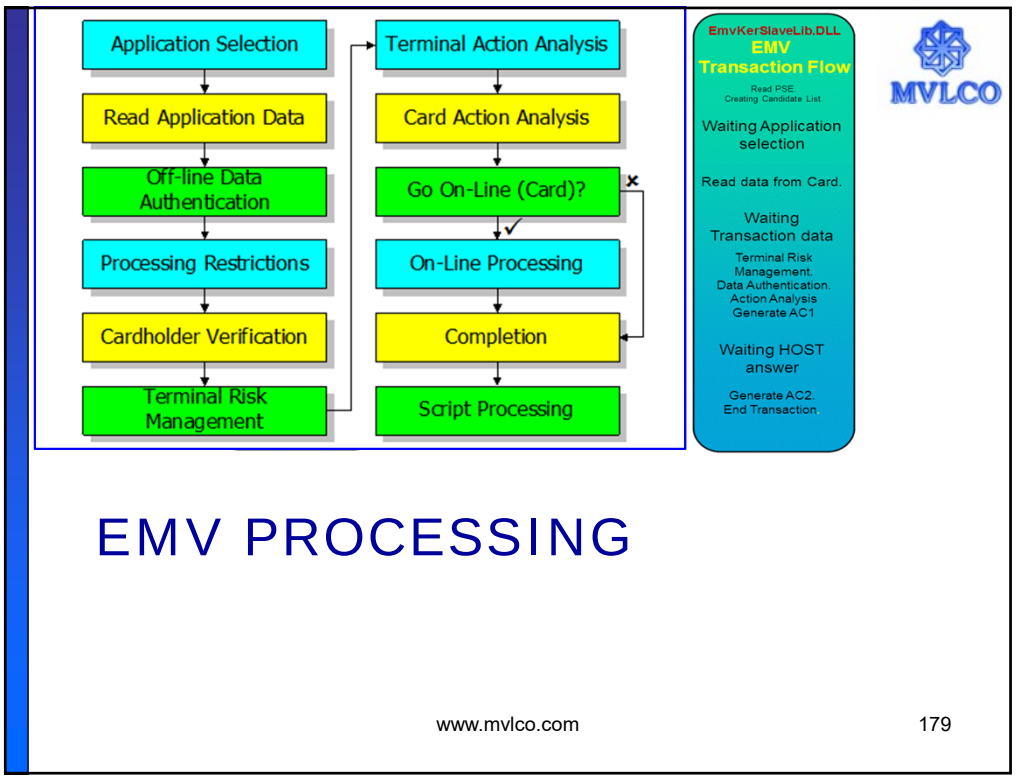
EMV AND NON-EMV ONLINE TRANSACTION PROCESSING

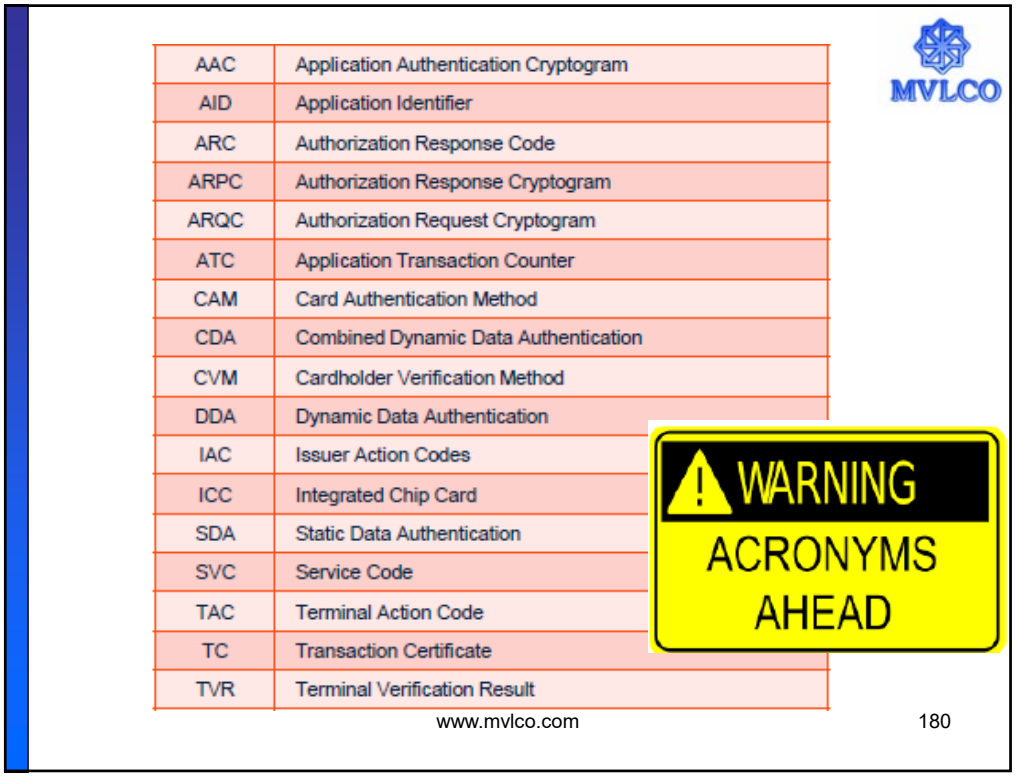
Concepts

- **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)
  - A **floor limit** is the amount of money above which credit card transactions must be authorised.
  - Floor limit for electronic transactions is usually set to Zero, meaning

floor limit	We maintain a zero-dollar Floor Limit on all Charges for our Merchants in the U.S., Puerto Rico, the U.S. Virgin Islands, or other U.S. territories and possessions. This means that we require an Authorization on all purchases, regardless of the amount.

EMV TRANSACTION PROCESSING





Card session summary

A card session is comprised of the following stages:

- Insertion of the ICC into the IFD and connection and activation of the contacts.
- Reset of the ICC and establishment of communication between the terminal and the ICC.
- Execution of the transaction(s).
- Deactivation of the contacts and removal of the ICC.

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 (Figure 17)
  - Application Identifier (AIDs) method (Figure 18)
  - Build candidate list
  - Final selection
- **Initiate application process (Figure 6)**
  - 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) (Figure 8)**
  - Offline PIN verification
  - Online PIN verification
  - Signature
  - Combined CVM
  - No CVM required and CVM Limits
- **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 (Figure 7)**
  - Details of card risk management algorithms within the ICC are specific to the issuer
  - Card cumulative total transaction amount limit (CTTAL)
  - 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.

THE COMPLETION PROCESS

DATA AUTHENTICATION SDA/DDA/CDA

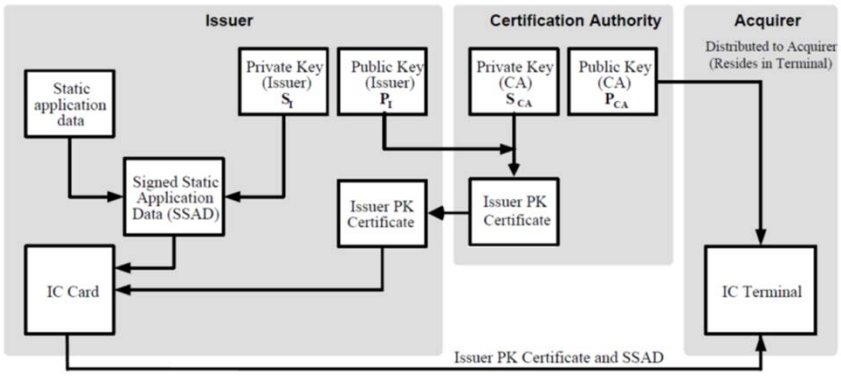
Static data authentication (SDA)

- Offline static data authentication is performed by the terminal using a digital signature scheme based on public key techniques to confirm the legitimacy of critical ICC-resident static data. This detects unauthorised alteration of data after personalisation.
- **SDA requires the existence of a certification authority, which is a highly secure cryptographic facility that 'signs' the issuer's public keys.**
- **Every terminal conforming to EMV specification shall contain the appropriate certification authority's public key(s) for every application recognised by the terminal.**
- EMV specification permits multiple AIDs to share the same 'set' of certification authority public keys.
- The terminal may support a Certification Revocation List (CRL) that lists the Issuer Public Key Certificates that payment systems have revoked.

SDA Process overview

- To support SDA, each terminal shall be able to store six certification authority public keys per Registered Application Provider Identifier (RID) and shall associate with each such key the key-related information to be used with the key (so that terminals can in the future support multiple algorithms and allow an evolutionary transition from one to another).
- The terminal shall be able to locate any such key (and the key-related information) given the RID and Certification Authority Public Key Index as provided by the ICC.
- **Three main steps in the SDA process are** :
  - Retrieval of the Certification Authority Public Key by the terminal
  - Retrieval of the Issuer Public Key by the terminal
  - Verification of the Signed Static Application Data by the terminal

RID List



Card provides to Terminal:
- Issuer PK Certificate (P_I signed by CA using S_{CA})
- Signed Static Application Data (SSAD) (signed by the Issuer using S_I)

Terminal:
- Uses P_{CA} to verify that the Issuer's P_I was signed by the CA
- Uses P_I to verify that the Card's SSAD was signed by the Issuer

Offline Dynamic Data Authentication (DDA/CDA)

Two forms of offline dynamic data authentication exist:

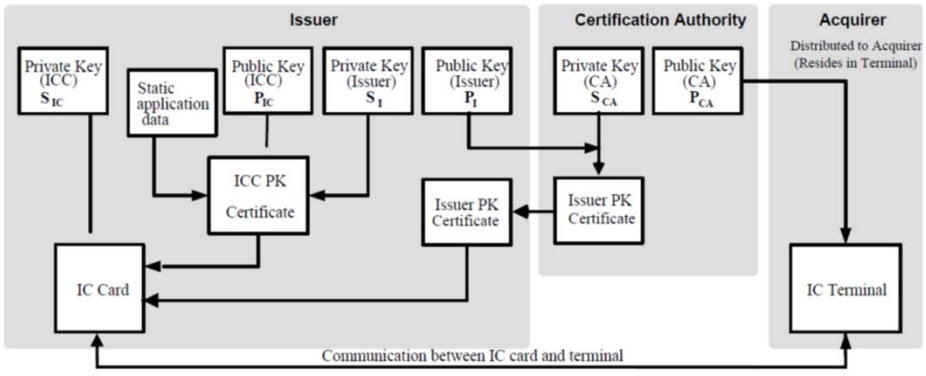
- **Dynamic Data Authentication (DDA) executed before card action analysis**, where the ICC generates a digital signature on ICC-resident/generated data identified by the ICC Dynamic Data and data received from the terminal identified by the Dynamic Data Authentication Data Object List (DDOL).
- **Combined Dynamic Data Authentication/Application Cryptogram**
- Generation (CDA) executed at issuance of the first and second GENERATE AC commands. In the case of a Transaction Certificate (TC) or Authorisation Request Cryptogram (ARQC), the ICC generates a digital signature on ICC-resident/generated data identified by the ICC Dynamic Data, which contains the TC or ARQC, and an Unpredictable Number generated by the terminal.
- The AIP denotes the options supported by the ICC.

www.mvlco.com 191

Key steps in DDA

- **The main steps in the DDA process are :**
  - Retrieval of the Certification Authority Public Key by the terminal
  - Retrieval of the Issuer Public Key by the terminal
  - Retrieval of the ICC Public Key by the terminal
  - Terminal issues INTERNAL AUTHENTICATE command : DDOL with the Unpredictable Number generated by the terminal
  - Dynamic signature generation and signing of data by ICC
  - Dynamic signature verification : apply the recovery function on the Signed Dynamic Application Data using the ICC Public Key in conjunction with the corresponding algorithm
- If all the above steps were executed successfully, DDA was successful.

www.mvlco.com 192



Card provides to Terminal:

- Issuer PK Certificate (P_I signed by the CA S_{CA})
- ICC PK Certificate (P_{IC} and static application data signed by Issuer S_I)
- Card and terminal dynamic data and digital signature (dynamic data signed by Card S_{IC})

Terminal:

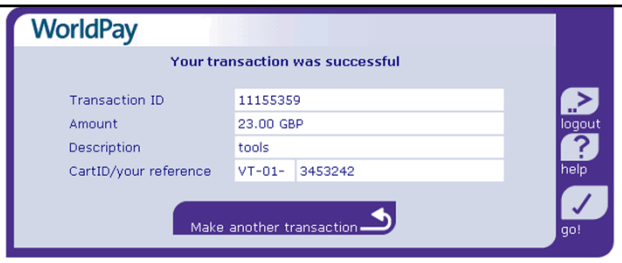
- Uses P_{CA} to verify that the Issuer's P_I was signed by CA
- Uses P_I to verify that Card P_{IC} and static application data were signed by Issuer
- Uses P_{IC} to verify the card's signature on the dynamic data

www.mvlco.com 193

Combined Dynamic Data Authentication (CDA)

- CDA consists of a dynamic signature generated by the ICC (similar to DDA but including Application Cryptogram (AC) generation) followed by verification of the signature by the terminal.
- It is applicable to both the first and second GENERATE AC commands and requires the retrieval of the relevant public keys as described earlier.
- Since the public keys are not required until the CDA signature is verified as part of processing the response to the first GENERATE AC, retrieval of the public keys may happen any time before verifying the CDA signature.

www.mvlco.com 194



AUTHENTICATION, ACCOUNTING, AUTHORISATION - AAA

CUSTOMER AUTHENTICATION

Authentication

- **Card present transactions (Electronic)**
  - PIN
  - Signature
- **Card not present transactions**
  - Online transactions
    - CVV2
    - One Time Password (OTP)
    - MasterCard SecureCode
    - Verified by VISA (VbV)
    - Adaptive authentication
  - **Phone transactions**
    - Address Verification Service (AVS)
    - IVRS/TPIN verification

MVLCO

I ♥ PIN

Chip and PIN

VERIFIED by VISA

MasterCard SecureCode for Online Merchants

Building Consumer Confidence, Extending Your Market Reach

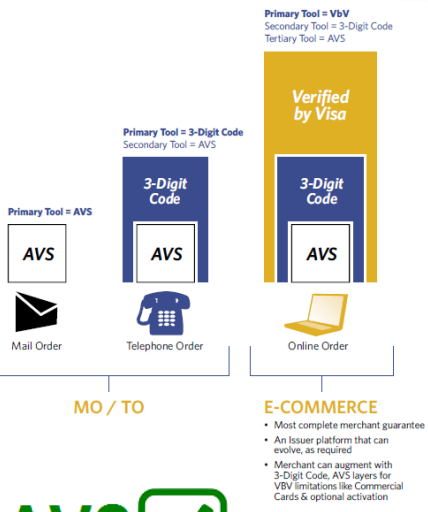
Multi-factor Authentication Channels

MVLCO

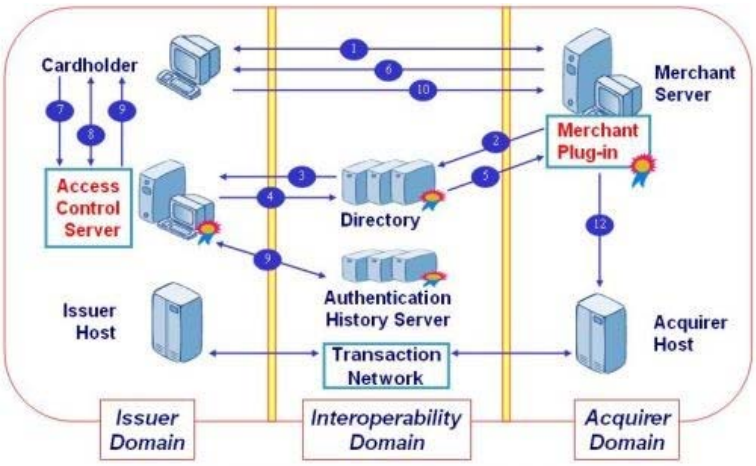
Authentication Channel	User Devices and Examples
Static password for Verified by Visa, MasterCard SecureCode, JCB J/Secure and American Express SafeKey.	Browser 
Mobile phone using: • SMS (instant or batch SMS) or • Mobile phone applets*.	Mobile Phone 

Multi-factor Authentication Channels

Authentication Channel	User Devices and Examples
Static passwor MasterCard Se American Expr	One-time password (OTP) device (various device vendors supported).	One Time Password Devices 
	EMV/CAP for MasterCard CAP, Visa DPA and JCB J/Smart.	CAP Compliant Chip Cards and Readers 
Mobile phone u • SMS (instar or • Mobile phor	Transaction Authorization Numbers (TAN) .	Scratch Card, TAN Lists, Printed Card or Bank Statements. 



========== RESULTS ========== AVS
Response : This transaction has been approved
Authorization Code : 209950
Address Verification : Street Address: Match -- First 5 Digits of Zip: Match



MVLCO

3D SECURE
VBV - SECURECODE

Stay secure when buying online

3D Secure
Verified by VISA
MasterCard SecureCode

MVLCO

What is 3-D Secure Payer Authentication?

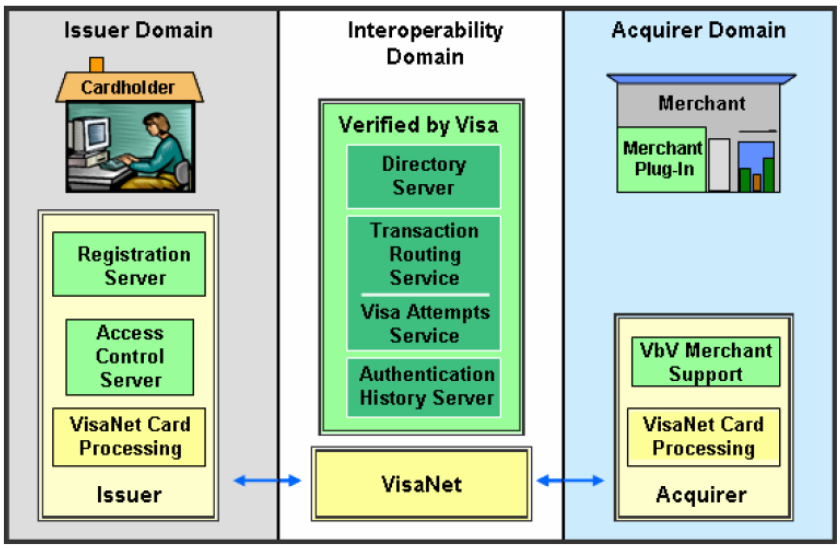
- Payer authentication enables **all** parties in an e-commerce payment transaction to transmit confidential and valid payment data, and provides verification to the merchant that the buyer is the authorized owner of a particular card account.
- Until recently, Internet based card transactions have been classified as 'card-not-present' and 'no signature present' so it has been virtually impossible to prove that the actual cardholder is the person performing the payment transaction at an Internet merchant site.
- **The result?** 78% of all e-commerce chargebacks are from 'unauthorised transaction' reason codes commonly referred to as the "I didn't do it" chargebacks.

Why have the Card Associations introduced 3-D Secure?

- This changes with the introduction of **3-D Secure™** services which provides Internet merchants with the ability to verify the consumer's true identity through a secure, electronic, non 'face-to-face' authentication process.
- To press the importance of eliminating card and chargeback fraud on Internet transactions the Card Associations have also instituted **chargeback liability shift** to protect merchants from online fraud and habitual chargeback offenders.
- 3-D Secure has been named by VISA and MasterCard because there are 3 interoperability domains involved in the authentication process.
  - Issuer Domain
  - Interoperability Domain
  - Acquirer Domain

Verified by VISA
MasterCard SecureCode

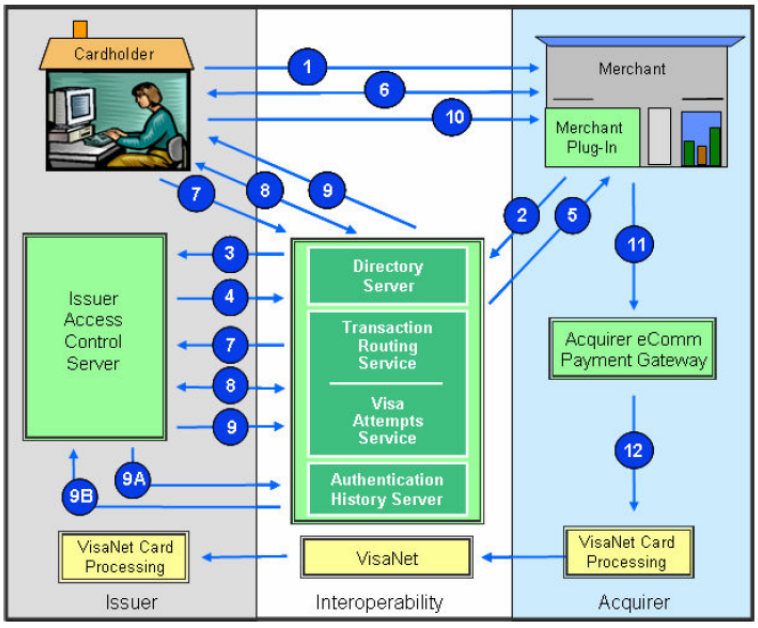
VbV Process



Two steps in VbV

- **Cardholder enrollment and personal assurance message**
- **Cardholder enrollment** or activation in the Verified by Visa program.
  - Cardholder advance registration/setup
  - Cardholder activation during shopping
  - Usage of adaptive authentication during enrollment
- **Cardholder authentication** during an online purchase at a participating merchant.
  - enter a password that is used for authentication
  - enter the requested information to verify their identity

Purchase transaction flow



Cardholder Authentication Verification Value (CAVV)

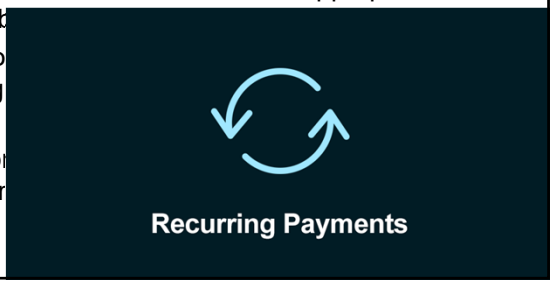
- The CAVV is a cryptographic value derived by the issuer during authentication that can provide evidence of the results of payment authentication during an online purchase.
- If a merchant receives a CAVV value in a Payer Authentication Response message from the issuer, the CAVV must be included in the VisaNet authorization message in order for the merchant to receive chargeback protection for U.S. and international transactions:
  - The merchant must be able to send the CAVV to its acquirer.
  - The acquirer must be able to receive the CAVV from the merchant and correctly transmit the data in the authorization request.

No Re-Use of Authentication Data

- Authentication data for a transaction must not be submitted in the Authorization Request for another transaction.
- There are **two exceptions** to this general requirement.
  - **Split Shipment**: A split shipment occurs when a single purchase order results in more than one shipment of merchandise. In the event a merchant splits the shipment of an order, the second Authorization Request may be submitted with the original authentication data for the purchase.
  - The total amount of the split transaction must not exceed 15% over the original authentication amount. The 15% variation allows for shipping costs associated with the items. Any authorization amount that exceeds 15% of the authenticated amount is not subject to Verified by Visa chargeback protection and may be charged back by the issuer.
  - **Delayed Delivery**: When a second Authorization Request is submitted for the same original purchase due to delayed delivery, the authentication data may be included in the second Authorization Request message.

Recurring transactions

- **Recurring transactions** occur when the cardholder and merchant agree to purchase goods or services on an ongoing basis over a period of time.
- Recurring transactions are multiple transactions processed at predetermined intervals, **not to exceed one year between transactions**.
  - To qualify for Verified by Visa chargeback protection, the first transaction in the series must be authenticated and must follow authorization rules associated with an authenticated transaction, which means the authorization is submitted with the appropriate ECI and CAVV for the Verified b
  - All subsequent authorizatio be processed as Recurring Indicator.
  - The merchant must not sto subsequent authorization tr



Installment Transactions

- Like **recurring transactions**, installment transactions are divided into two or more transactions and are billed to an account in multiple segments over a period of time that is agreed to by the cardholder and merchant.
- However, the transaction **is for a single good or service rather than an ongoing (or recurring) purchase. The transactions must have a specified end date.**
- Similar to the processing of recurring payments, the initial installment transaction must be authenticated and must follow authorization rules associated with an authenticated transaction.
- The remaining transactions are processed as installment transactions, so must not contain authentication data.

No chargeback liability : merchants

- In USA, there are **four Merchant Category Codes** (MCCs) for which merchants **retain chargeback liability** when cardholders are either authenticated with Verified by Visa or there is an attempted Verified by Visa authentication. These four Merchant Category Codes are:
  - Wire Transfer/Money Order (MCC 4829)
  - Direct Marketing-Inbound Teleservices (MCC 5967)
  - Non-Financial Institution-Foreign Currency, Money Order (not Wire Transfer), Travelers' Cheques (MCC 6051)
  - Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting and Wagers at Race Tracks (MCC 7995)
- The chargeback liability for the above four MCCs does not apply to international transactions where either the cardholder or merchant is non-U.S.


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/B6C2555EA87911C7
Merchant ID: 70726362
Terminal ID: 2310748
TVR : 0080008000
TSI : F800
Captured : CHIP
Cust. Ver. : 412302
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.

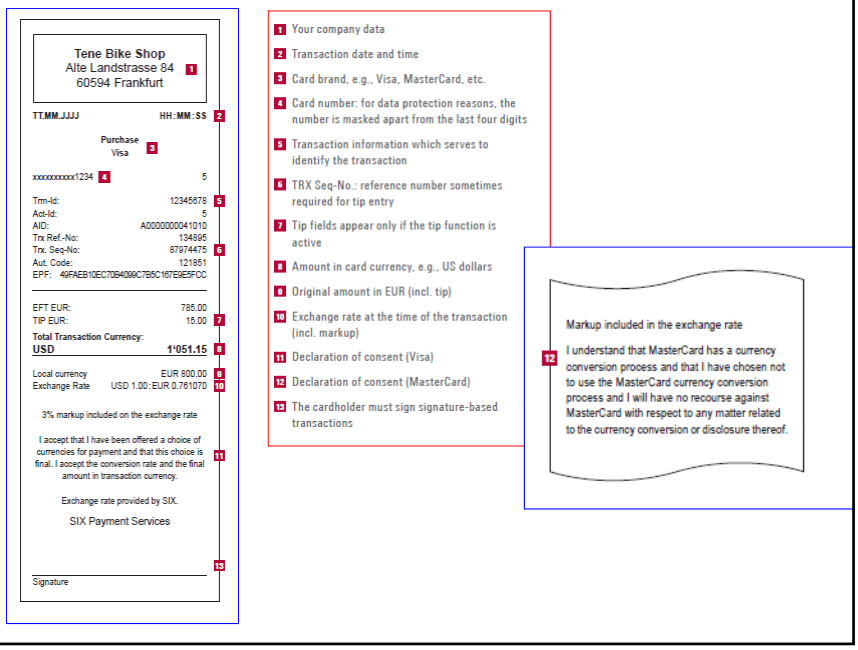
About Customer Preferred Currency

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.

What is DCC or CPC ?



What is DCC or CPC ?

Currency converter

My Card is in

(INR) Indian Rupee

My Transaction was in

(USD) United States Dollar

Enter conversion fee (0-10%) 1.00 %

Your payment service provider may or may not apply currency conversion fees. Refer to your issuer's terms and conditions to find out more about this.

Transaction date

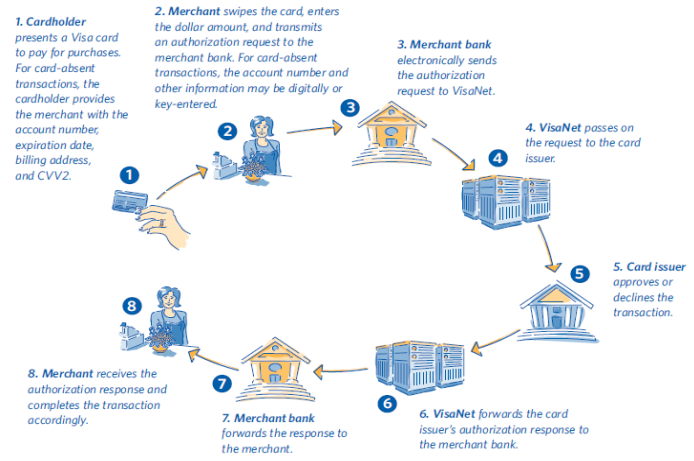
24/03/2016

Purchase amount

100.00

Calculate exchange rate

Authorization



ACCOUNTING AND AUTHORISATION

Recall!! Authorisation

- An **authorization** is an approval on a cardholder account for a sale amount.
- An **authorization hold** is a reduction of the cardholder's credit line for the amount of the sale. This hold can remain on the cardholder's account for up to 30 days, depending upon the issuing bank policy.
- **Authorisation**
  - Original authorisation
  - Replacement authorisation
  - Resubmission authorisation
  - Supplementary authorisation

Authorisation decisions (1)

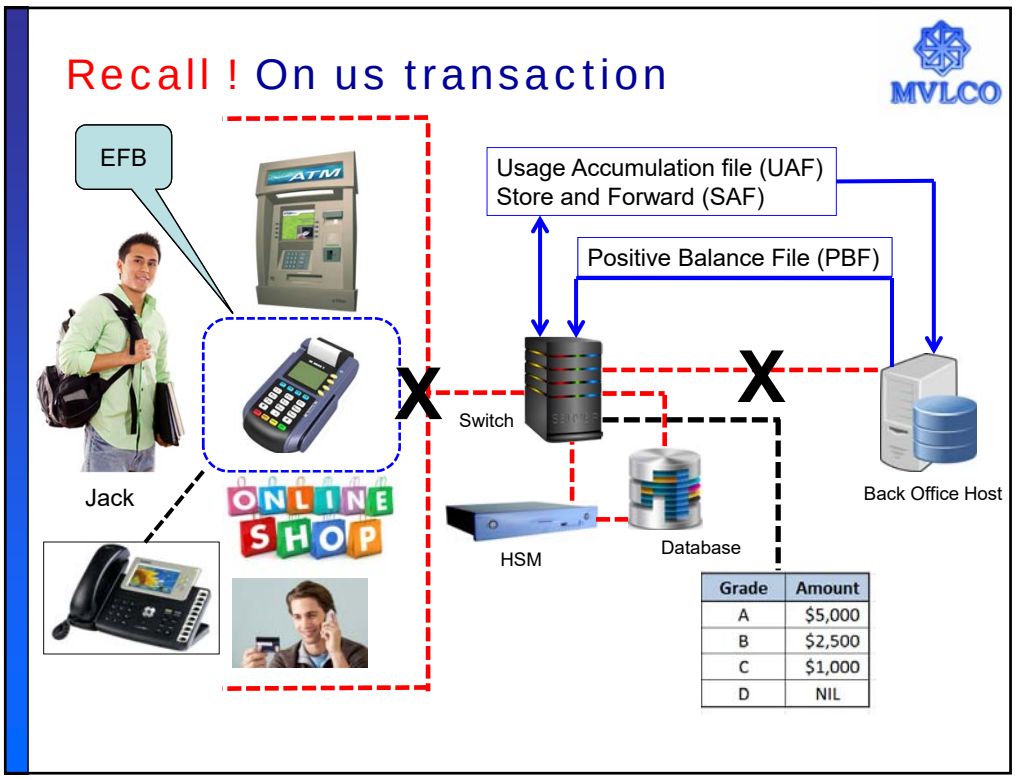
- Full approval
- Partial approval
- Declined or rejected
- **Referral** (the card issuer is requesting direct contact with the business in order to authorize the sale.)
- **Hold card/Call center.** Indicates that the card issuer is requesting the card be removed from circulation.
- **Call center.** This response indicates the card issuer is requesting direct contact with the business in order to authorize the sale.
- **Invalid account number.** The cardholder account number entered was incorrect.

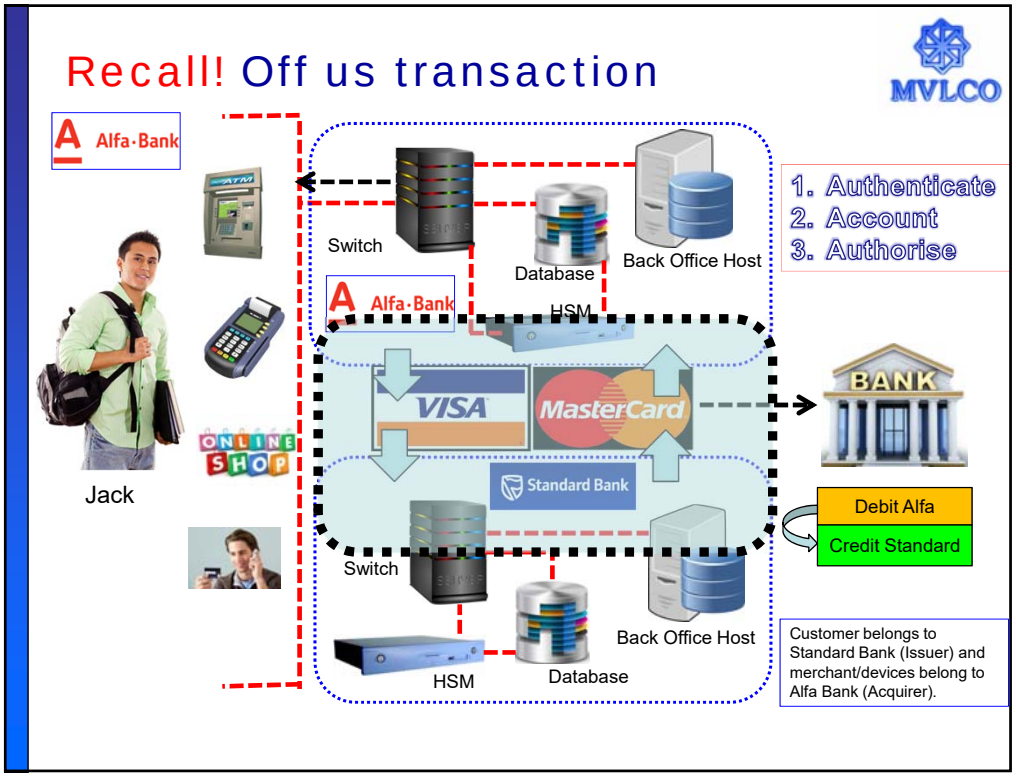
Authorisation decisions (2)

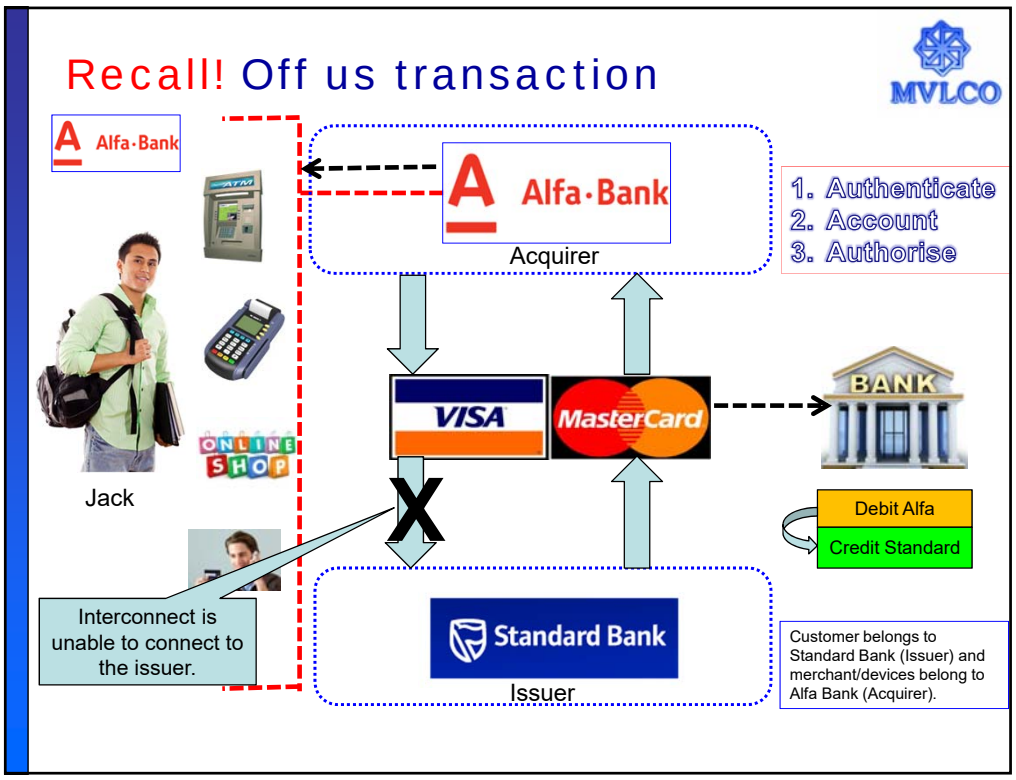
- **Invalid merchant number.** The network does not recognize the merchant account number.
- **Pick up card.** This indicates the card issuer wants the card out of circulation. Normally the response indicates a lost or stolen card.
- **Waiting for line.** Indicates that the phone lines are currently busy. The terminal will connect with the next available line.
- **Unable to connect.** Indicates there is a problem with the equipment or the network.
- **Code 10 operator.** If a transaction is suspicious or appears to be fraudulent, contact the authorization center and request a Code 10 Operator. A Code 10 Operator will make an outbound call to the issuing bank of the credit card. The issuing bank may request to speak directly with the cardholder for verification of information on their account.

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







Interconnect authorisation processes including STIP process (1)

MVLCO

- **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.

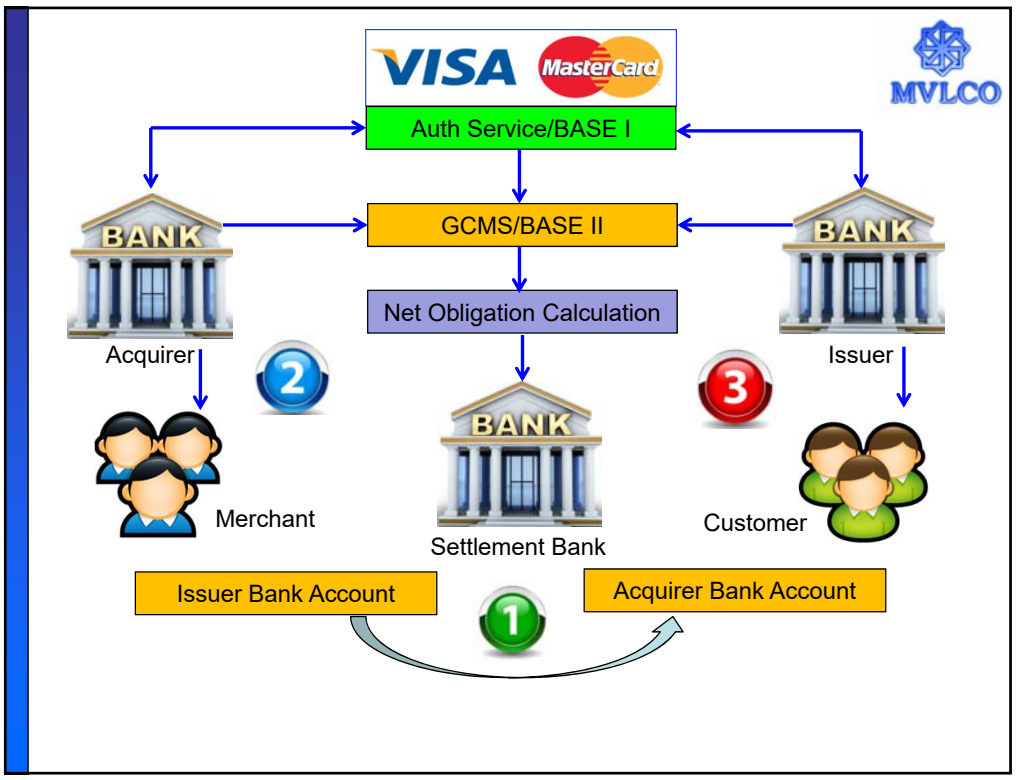
Files for STIP authorisation (1)

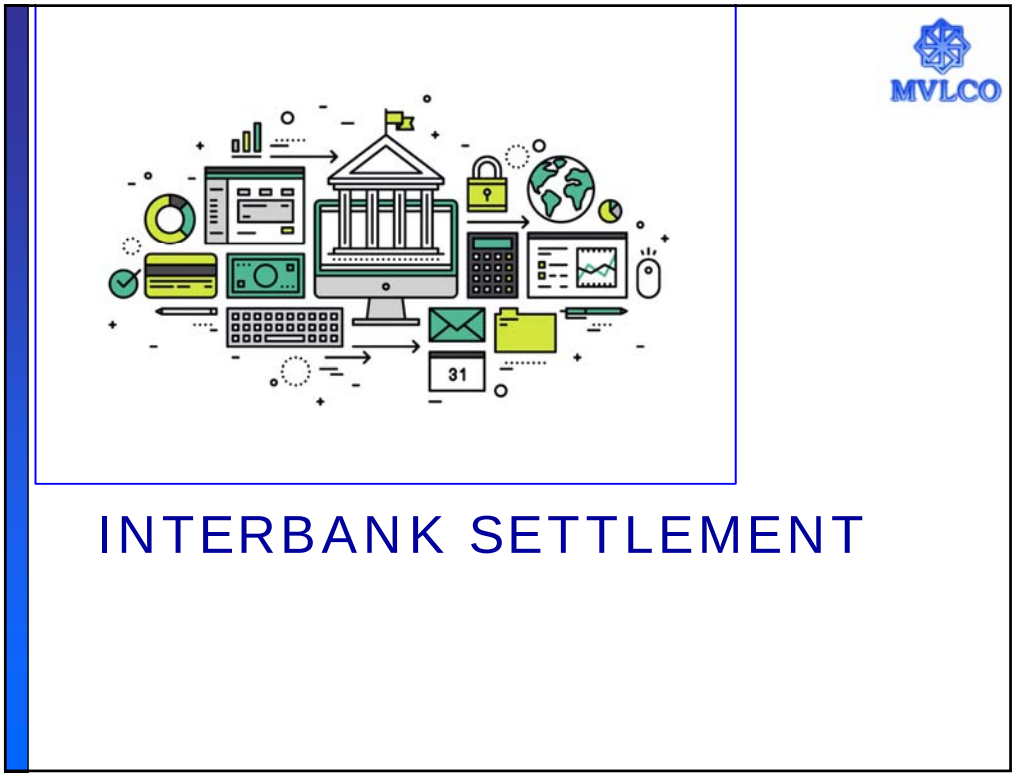
- **Authorization Processor (AP) Positive File**
  - Upload all cardholder records on the interconnect system.
  - Transactions are authorized for any valid card number, without a negative status, on the cardholder file.
  - All decisions are subject to multiple client-defined authorization parameters.
  - Daily dollar limit and velocity checks are available to limit activity and may be set at different levels depending on whether issuer's system is available or unavailable.
- **Positive File with Account Balances**
  - Account balances are refreshed daily using a batch file transmission from issuer's system.

Files for STIP authorisation (2)

- **Processor Interface (PI) Negative File**
  - Transactions are authorized for any valid card number that is not on the Negative File and subject to daily dollar limits.
  - In stand in, transactions are authorized for any valid card number that is not on the Negative File with a "hot card" or "blocked" status and has passed pre-defined edit checks such as PIN verification and expiration date checking.
  - Daily dollar limit checks are available to limit activity for all cardholders.
- **Exception File**.
  - Same as the PI Negative File however, exceptions are made for cardholders that require special limits (e.g., VIPs).

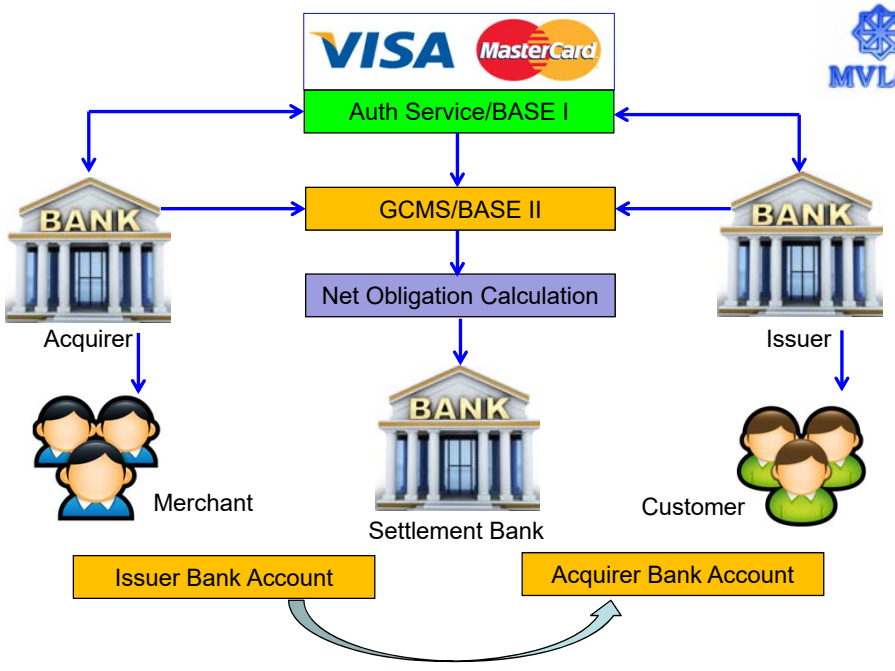
PAYMENT CYCLES





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.

MERCHANT TRANSACTIONS AND PRESENTMENT

Merchant transactions

- Sale
  - Tab processing
- Void/reversal – before settlement
- Refund processing – no cash refund
- Cash out
- MOTO transaction
- Preauthorisation hold
- Shift report
- Deposit time limits – as specified by the acquirer
- Tip/gratuity processing
- Split tender processing
- Deposit and balance amount authorisation
- Convenience fee

Tip authorisation

- Tip is permitted to be added only if the POS has such a facility.
- Acquirers generally put a limit (say 20%) of the transaction amount as tip/gratuity.
- Authorisation can be obtained
  - With tip included initially
  - With tip added subsequently.

Restaurants are permitted and protected from chargeback for failure to obtain proper authorization if they clear for an amount up to 20 percent more than they authorized, and the same is true up to 15 percent additional for hotel, car rental, and cruise line merchants. For car rental, this threshold is the greater of 15 percent or $75.00.

Split tender transaction/ partial authorisation

- A card holder may purchase goods/services partly by using card and partly using some other mode of payment.
- For instance, a customer purchases a laptop for USD 5,000, uses credit card for USD 4,000 and balance is paid in cash.

- Partial authorisation is obtained when the balance limit is not sufficient to cover the transaction completely.
- For instance, a customer purchases a laptop for USD 5,000, swipe his credit card for USD 5,000. The transaction is declined as the available limit is only USD 4,000. The merchant can seek a partial authorisation of USD 400 and balance is paid through alternative mode.

Delayed delivery transactions

- Some merchandise, requires delivery sometime after the transaction date. In these delayed-delivery situations, the customer pays a deposit at the time of the transaction and agrees to pay the balance upon delivery of the merchandise or services.
- To complete such transaction, the merchant has to :
  - Create two transaction receipts, one for the deposit and one for the balance. Write, print out, or stamp “Deposit” or “Balance,” as appropriate, on the receipt.
  - Obtain an authorization for each transaction receipt on their respective transaction dates..
  - Ensure that “Delayed Delivery” is written, printed, or stamped along with the authorization code, on each transaction receipt.
- The merchant may deposit the deposit portion of the transaction before delivery of the goods or services. However, he must not deposit the balance portion of the transaction amount prior to delivery.

Surcharge and convenience fee

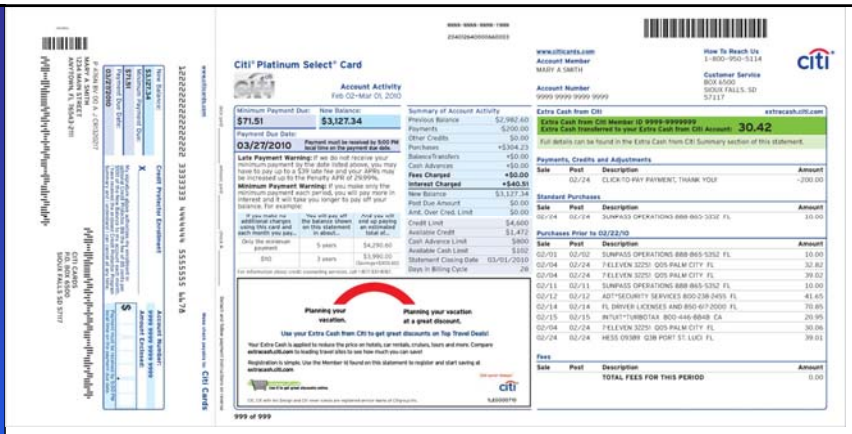
- A surcharge is…
  - A charge assessed by the merchant to the consumer for the payment service itself. (VISA) A surcharge is…
  - Any fee charged in connection with a transaction that is not charged if another payment method is used. (MasterCard)
  - **"Surcharges are prohibited by both VISA and MasterCard but merchants are allowed to offer a Discount for Cash*"**
- VISA: a convenience fee can be levied for a cardholder's use of a special service rendered at the time payment is made. Unlike a surcharge, a convenience fee is not a charge for the payment service itself, but is a fee linked with the transaction such as the use of a Voice Response Unit (VRU).
- MasterCard: a merchant is permitted to charge a fee (such as a bona fide commission, postage, expedited service or convenience fee, and the like) the fee is imposed on all like transactions regardless of the form of payment used.

General rules for convenience fees

- Merchant must provide bona fide convenience in the form of an alternative payment channel outside the merchant's customary payment channels.
- The alternative payment channel must be in a non-face-to-face environment. (Normal non face to face merchant may NOT charge a convenience fee)
- Convenience fee must be included in the transaction (cannot be a separate transaction).
- Convenience fee must be disclosed to the customer prior to the completion of the transaction.
- Consumer must have the ability to cancel the transaction if they do not want to pay the convenience fee.
- The same convenience fee must apply to all forms of payment accepted in the alternative payment channel.

General rules for convenience fees

- The convenience fee must be a flat or fixed amount regardless of the amount due to the merchant for goods and services purchased.
- Utility Payment Program merchants are Excluded from charging convenience fees.
- Recurring payment transactions are ineligible from charging convenience fees.
- Merchant must provide actual goods and services to a cardholder to be able to charge a convenience fee.
- A convenience fee may not be charged by ANY third party.



CUSTOMER BILLING AND PAYMENT

Balance computation and finance charge

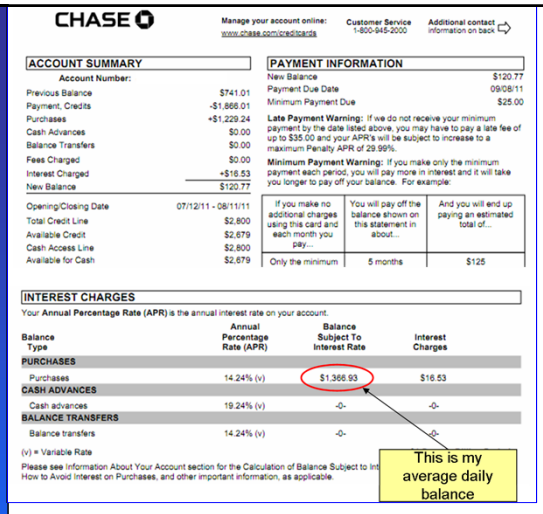
- Regulation may prescribe methods of calculating balances and computing finance charge.

Title 12 → Chapter X → Part 1026

Browse Previous | Browse Next

Title 12: Banks and Banking

PART 1026—TRUTH IN LENDING (REGULATION Z)



CHASE

Manage your account online: www.chase.com/creditcards
Customer Service 1-800-945-2000
Additional contact information on back

ACCOUNT SUMMARY

Account Number:

Previous Balance	$741.01
Payment, Credits	-$1,866.01
Purchases	+$1,229.24
Cash Advances	$0.00
Balance Transfers	$0.00
Fees Charged	$0.00
Interest Charged	+$16.53
New Balance	$120.77
Opening/Closing Date	07/12/11 - 08/11/11
Total Credit Line	$2,800
Available Credit	$2,679
Cash Access Line	$2,800
Available for Cash	$2,679

PAYMENT INFORMATION

New Balance	$120.77
Payment Due Date	09/08/11
Minimum Payment Due	$25.00

Late Payment Warning: If we do not receive your minimum payment by the date listed above, you may have to pay a late fee of up to $35.00 and your APR's will be subject to increase to a maximum Penalty APR of 29.99%.

Minimum Payment Warning: If you make only the minimum payment each period, you will pay more in interest and it will take you longer to pay off your balance. For example:

If you make no additional charges using this card and each month you pay...	You will pay off the balance shown on this statement in about...	And you will end up paying an estimated total of...
Only the minimum	5 months	$125

INTEREST CHARGES

Your **Annual Percentage Rate (APR)** is the annual interest rate on your account.

Balance Type	Annual Percentage Rate (APR)	Balance Subject To Interest Rate	Interest Charges
PURCHASES			
Purchases	14.24% (v)	$1,366.93	$16.53
CASH ADVANCES			
Cash advances	19.24% (v)	-0-	-0-
BALANCE TRANSFERS			
Balance transfers	14.24% (v)	-0-	-0-

(v) = Variable Rate

Please see Information About Your Account section for the Calculation of Balance Subject to Int
How to Avoid Interest on Purchases, and other important information, as applicable.

This is my average daily balance

PERIODIC STATEMENT

Periodic statement (1) Contents

- **Previous balance**. The account balance outstanding at the beginning of the billing cycle.
- **Identification of each credit transactions** viz. sale credit and non-sale credit.
- **Periodic rates used to compute the interest charge** expressed as an annual percentage rate and using the term Annual Percentage Rate, along with the range of balances to which it is applicable.
- The amount of the balance to which a periodic rate was applied and an explanation of how that balance was determined, using the term **Balance Subject to Interest Rate**.

Periodic statement (2) Contents

- **Interest**. Finance charges attributable to periodic interest rates, using the term *Interest Charge,* must be grouped together under the heading *Interest Charged,* itemized and totaled by type of transaction, and a total of finance charges attributable to periodic interest rates, using the term **Total Interest**, must be disclosed for the statement period and calendar year to date.
- **The closing date** of the billing cycle and the account **balance outstanding on that d**ate.
- **Due date and late payment costs**. The due date disclosed shall be the same day of the month for each billing cycle.
- **Grace period**.
- **Address for notice of billing errors**.

Minimum payment warning

- A statement with a bold heading: "**Minimum Payment Warning: If you make only the minimum payment each period, you will pay more in interest and it will take you longer to pay off your balance**;"
- The minimum payment repayment estimate, If the minimum payment repayment estimate is less than 2 years, the card issuer must disclose the estimate in months. Otherwise, the estimate must be disclosed in years and rounded to the nearest whole year;
- The minimum payment total cost estimate,
- A toll-free telephone number where the consumer may obtain information about credit counseling services
- Estimated monthly payment for repayment in 36 months

PAYMENTS

Payments

- **USA Example:**
- A creditor shall credit a payment to the consumer's account as of the date of receipt, except when a delay in crediting does not result in a finance or other charge.
- A creditor may specify reasonable requirements for payments that enable most consumers to make conforming payments.
- Payments on made in person at a branch or office of a card issuer that is a financial institution prior to the close of business of that branch or office shall be considered received on the date on which the consumer makes the payment.
- A card issuer that is a financial institution shall not impose a cut-off time earlier than the close of business for any such payments. However, a card issuer may impose a cut-off time earlier than 5 p.m., if the close of business of the branch is earlier than 5 p.m.

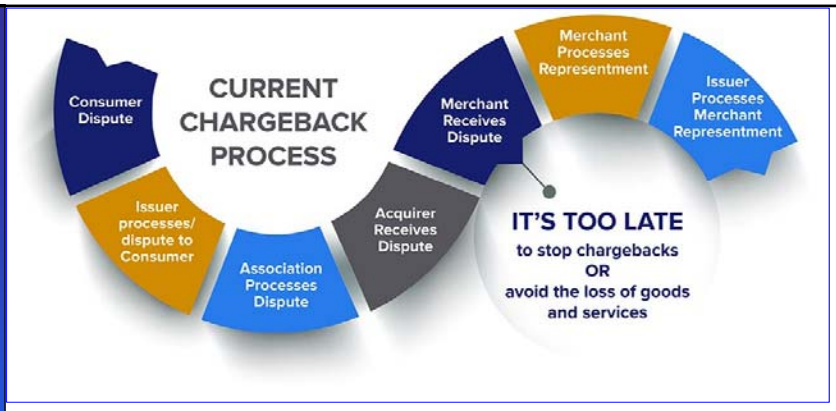
TREATMENT OF CREDIT BALANCES; ACCOUNT TERMINATION

Treatment of credit balances

- **USA Example:**
- When a credit balance in excess of $1 is created on a credit account, the creditor shall:
  - Credit the amount of the credit balance to the consumer's account;
  - **Refund** any part of the **remaining credit balance within seven business days** from receipt of a written request from the consumer;
  - Make a good faith effort **to refund** to the consumer by cash, check, or money order, or credit to a deposit account of the consumer, any part of the **credit balance remaining in the account for more than six month**s.
  - No action is required if the consumer's current location is not known to the creditor and cannot be traced through the consumer's last known address or telephone number.

Account termination and inactive account

- **USA Example:**
- A creditor shall not terminate an account prior to its expiration date solely because the consumer does not incur a finance charge.
- A creditor may terminate an account that is inactive for three or more consecutive months. An account is inactive if no credit has been extended (such as by purchase, cash advance or balance transfer) and if the account has no outstanding balance.



MVLCO

BILLING ERRORS AND CHARGEBACKS

What is an error and related inquiry?

MVLCO

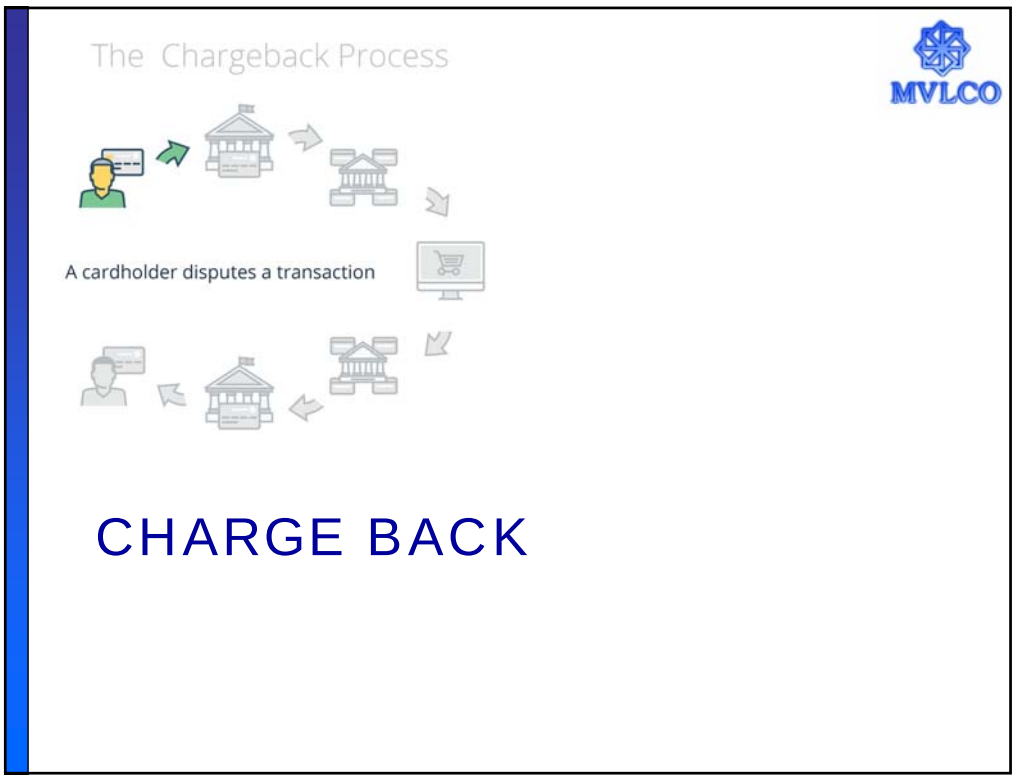
- **An error means:**
  - An unauthorized electronic fund transfer;
  - An incorrect electronic fund transfer to or from the consumer's account;
  - The omission of an electronic fund transfer from a periodic statement;
  - A computational or bookkeeping error made by the financial institution relating to an electronic fund transfer;
  - The consumer's receipt of an incorrect amount of money from an electronic terminal;
  - An electronic fund transfer not identified

Notice of error from customer (1)

- **Example USA:**
- An FI may receive **an oral or a written notice of error** from the consumer **no later than 60 days** after the institution sends **the periodic statement** or provides **the passbook** documentation, **on which the alleged error is first reflected**. A financial institution may require the consumer to give **written confirmation of an error within 10 business** days of an oral notice
- When a **notice of error is based on documentation or clarification that the consumer requested earlier from the FI**, the consumer's notice of error is timely if received by the FI no later **than 60 days** after the FI sends the information requested.

Notice of error from customer (2)

- **Example USA:**
- An FI shall **investigate** promptly and shall determine whether an error occurred **within 10 business days** of receiving a notice of error. The institution shall **report the results** to the consumer **within three business days** after completing its investigation. The institution shall **correct the error within one business day** after determining that an error occurred.
- If the FI is unable to complete its investigation within **10 business days**, the institution may take **up to 45 days** from receipt of a notice of error to investigate and determine whether an error occurred.



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

mastercard

Chargeback Guide

16 January 2018

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

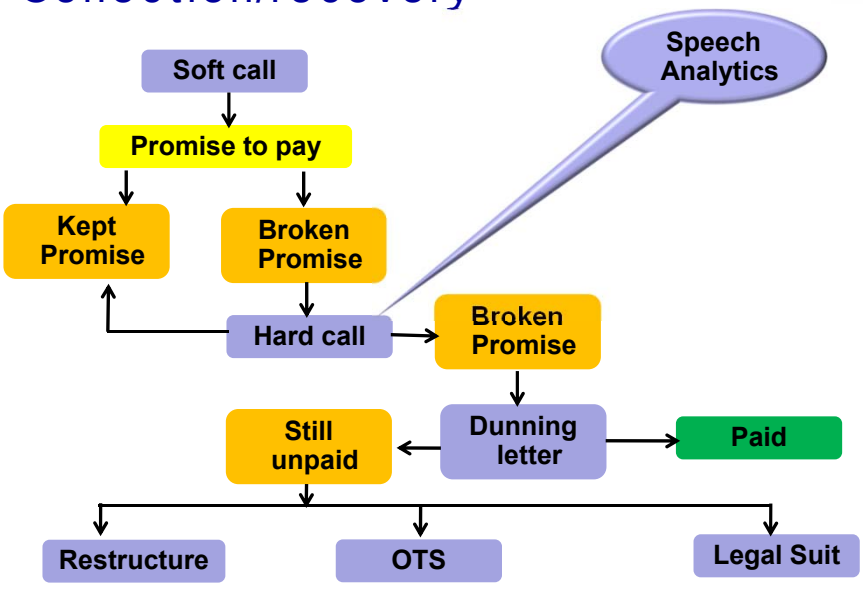
ID#: 081010-010410-0002445

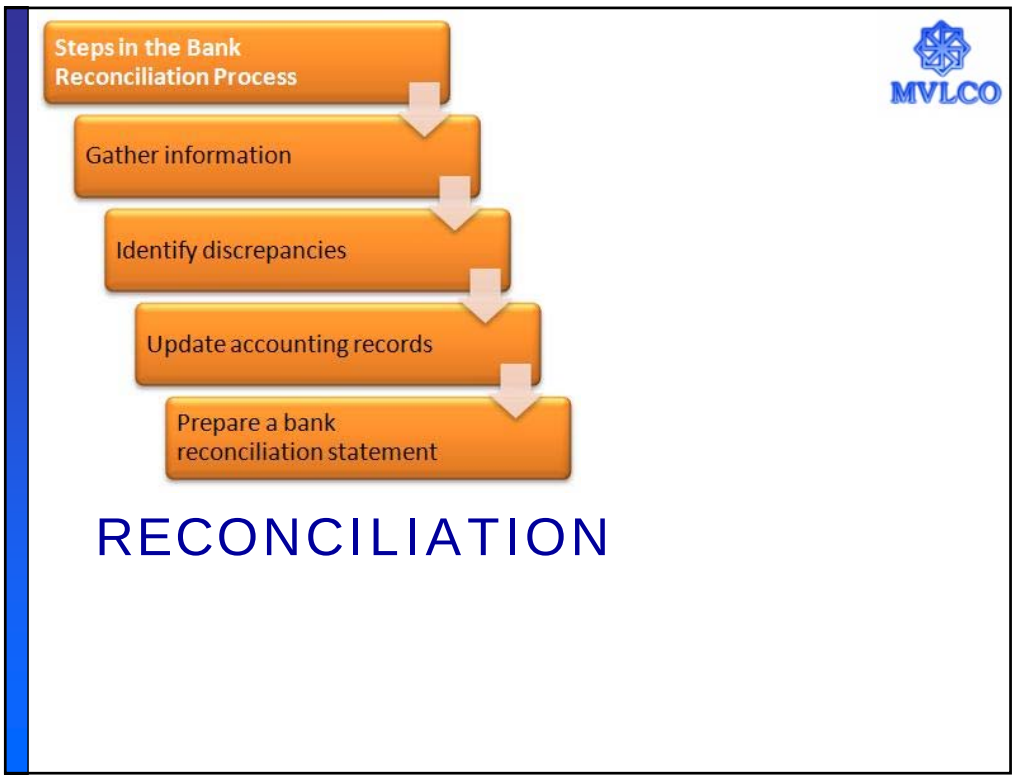
Termination of Merchant Agreement

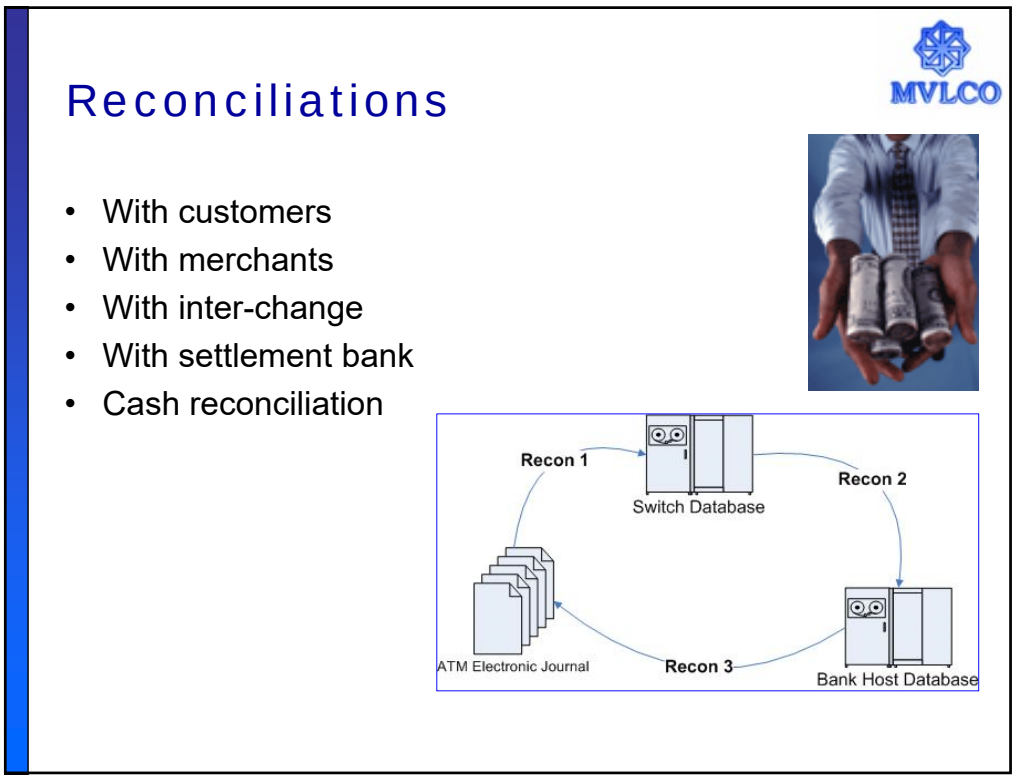
After verifying that Visa has prohibited a Merchant or Sponsored Merchant from participating in the Visa or Visa Electron Program, an Acquirer must terminate the Merchant Agreement no later than the date specified by Visa.

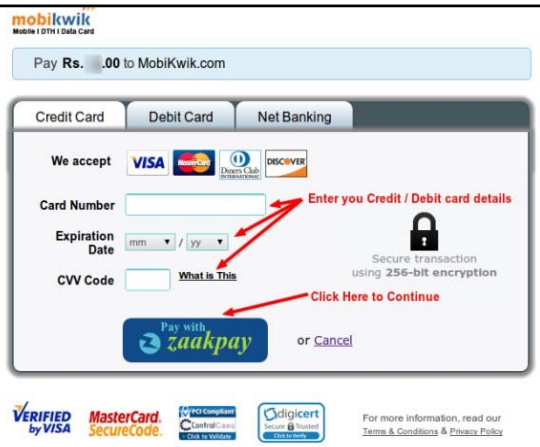
COLLECTION AND RECOVERY

Collection/recovery









MVLCO

REVENUE STREAMS

Who makes money ?

MVLCO

- Issuers
- Acquirers
- Processors
- Interchange agencies

HOW ?

  - By taking it from the merchants
  - By taking it from the customers

How are the merchant charged ?

- **Merchants pay "Merchant Discount".**
  - The rate charged to a merchant by a bank for providing debit and credit card services. The rate is determined based on factors such as volume, average ticket price, risk and industry. The merchant must set up this service with a bank, and agree to the rate prior to accepting debit and credit cards as payment.
  - Merchant discount includes interchange fees, association dues, network access charges and profit for the merchant service provider.
- **Components of merchant fees**
  - **Percentage Fee:** is charged as a percentage of a gross credit card transaction.
  - **Transaction Fees :** are charged when a merchant performs a transactions. a transaction is any action that requires communication with the processing bank. Clearing a batch, refunding a credit card order and other tasks are all considered transactions.
  - **Flat fees:** are charged regardless of processing volume or transaction activity and are the same amount each time they're charged. Monthly merchant account statement fees, membership fees and contract cancellation fees are examples of a flat fee.
- **Monthly minimum**

How are the merchant charged ?

- **Interchange Reimbursement Fees :** Acquirer pays to interchange and issuer
- **Reverse interchange fees :** Issuer pays acquires (for instance ATM)
- **Tiered pricing**
  - **Three Tier Merchant Account Rate Structure**
    - Qualified Discount Rate (lowest)
    - Mid Qualified Surcharge
      - (Qualified discount + Mid Qualified Surcharge = Final rate)
    - Non Qualified Surcharge
      - (Qualified discount + Non Qualified Surcharge = Final rate)
  - **Six-Tier Merchant Account Rate Structure**
    - Same structure as above. Only Credit and debit transaction are separated.

How are the customers charged? (1)

- **Basic fee**
  - Admission/application fee
  - Account setup/program fee
  - Annual membership fee
  - Additional card fee
- **Usage fee**
  - ATM/Debit card service fee
  - Purchase fee
  - Balance transfer fee
  - Cash advance fee
  - Foreign transaction fee
  - Expedited payment fee
  - Payment protection fee
  - Dormancy and inactivity fee
- **Interest and related fees**
  - Annual percentage rate (APR)/ finance charges
  - Payment skip option fee
  - Balance transfer APR
  - Penalty APR
- **Customer service fee**
  - Internet access fee
  - Paper statement fee
  - Account research fee
  - Charge for copies
- **Reward related fee**
  - Reward redemption fees
  - Reward recovery fee

How are the customers charged? (2)

- **Penalty charges**
  - Late payment fee
  - Over limit fee
  - Returned payment fee
- **Indirect benefits**
- **Breakage and float**
  - **Float** : the redemption of the rewards long after the purchase is made
  - **Breakage**: points earned but never redeemed.
- **Spoilage**
  - Balance of unused prepaid cards

MVLCO

COSTS

Costs

MVLCO

- Operational expenses
- Card production expenses
- Inter-connect charges
- Losses

- **Loyalty programs**
- Reward points
  - Flat or tiered
- Cash back programs
- Other benefits
- **Reward redemption**

Costs

MVLCO

- Premium Travel Privileges
- Exclusive Lifestyle Privileges
- Exclusive Dining Privileges
- Best-in-class Rewards Programme
- Preferential Financial Benefits
- Priority Customer Service
- Unparalleled Protection
- Terms and Conditions

Costs

MVLCO

1) Complimentary Taj Epicure Plus Membership

Indulgence just got redefined. The HDFC Infinia Credit Card introduces you to the exclusive Taj InnerCircle Gold and Epicure Plus membership. As a primary card holder, you will be enrolled for both programs once you use your Card. These complimentary memberships offer you special privileges at the Taj Hotels and Resorts, some of which are:

- 2.5 Epicure Points (each point is worth Rs 10) for every Rs 100 spent (net of taxes) at participating restaurants. You may redeem these points for fine dining experiences and exotic holidays at the Taj, or to offset stay and dining bills.
- One Taj InnerCircle Point for every Rs 80 spent on a room at Taj hotels around the world
- Happy Hours at the participating bars (6 pm-8 pm), any evening of the week, for a group of up to six people
- A set of gift certificates (valid for a year) for:
  - A complimentary round of drinks on any evening of the week
  - 50% discount on a buffet lunch at a Taj Coffee Shop from Monday to Saturday, and, two weekends at half rates at select hotels

Certified International Payment Systems Professional (CIPSP)™

Module 6
Card Frauds, PCI DSS and EMV Standards

MVL Consulting Private Limited
www.mvlco.com

Module Objective

At the end of this module, you will understand:

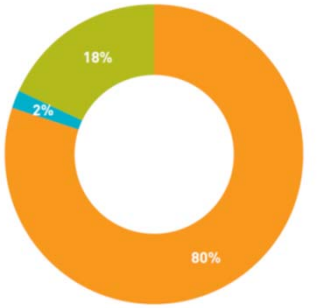
1. *Card frauds – examples*
2. *Payment Card Industry Data Security Standard (PCIDSS)*
3. *EMV Standards*

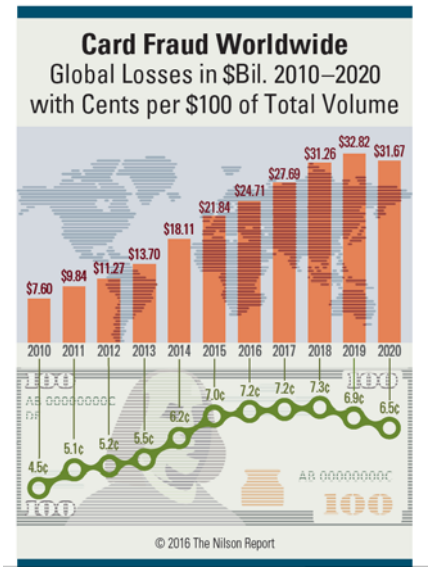
MVLCO

CARD FRAUDS

MVLCO

Card payment frauds





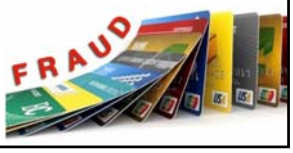
Why focus on credit cards ?

- Credit cards are responsible for $2.5 trillion in transactions a year at more than 24 million locations in 200 countries and territories.
- It is estimated that there are 10,000 credit card payment transactions every second around the world.
- Card fraud costs the U.S. $8.6 billion annually and the bulk of that loss falls on the card issuers.
  - (Source: Aite Group LLC)

Method	Percentage
Lost or stolen card	48%
Identity theft	15%
Skimming (or cloning)	14%
Counterfeit card	12%
Mail intercept fraud	6%
Other	5%

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 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.

Quick Statistics

- ▶ **$45 Million-** Total amount stolen
- ▶ **40,500-** ATM Withdrawals
- ▶ **27-** Countries where ATMs and money trails led to
- ▶ **17-** prepaid cards used in the two operations
- ▶ **2,904-** ATM withdrawals during a 10 hour swindling operation in Manhattan.

#CYBER CRIME JANUARY 30, 2018 / 3:50 AM / 7 DAYS AGO

'Jackpotting' hackers steal over $1 million from ATMs across U.S.: Secret Service

Dustin Volz 3 MIN READ

WASHINGTON (Reuters) - A coordinated group of hackers likely tied to international criminal syndicates has pilfered more than $1 million by hijacking ATM machines across the United States and forcing them to spit out bills like slot machines dispensing a jackpot, a senior U.S. Secret Service official said on Monday.

Jackpotting: hackers are making ATMs give away cash

Two of world's largest cash machine makers and US Secret Service warn of attacks that empty ATMs at rate of 40 notes per 20 seconds

Cybercriminals are hacking cash machines to force them to give out money in what is known as "jackpotting", according to two of the world's largest ATM makers and the US Secret Service.