D&B Learning Solutions

ADV-BN301

Cards

Cards

1. Card Landscape

a. Evolution of Cards

The cards industry has grown phenomenally in the last two decades and has become a strong substitute for cash. This is often referred to as plastic money. However, there are certain countries that have a huge parallel economy, where today, a large chunk of financial transactions happen in cash. This is because card transactions leave sufficient financial trails that enable traceability of fund flow.

Diners Club and American Express were the two early birds in this financial space. The credit of issuing the first credit card goes to Diner's Club which was introduced in 1951.

The backbone of Card processing is the settlement mechanism. In the early days this process was a purely manual one. Burgeoning volumes as well as evolving technology has brought drastic changes to the processing environment.

The diverse business needs have moved the card industry from credit and debit cards to other segments such as petro cards, frequent flyer cards, integrated transport system cards where a customer using a single card can purchase a metro/railway ticket as well as bus tickets. This model is widely prevalent in Singapore.

Business innovation has no boundaries. Although it is too early to comment on the technical details, the ambitious UID (Unique Identity) project of the Government of India may culminate into a Smart Card. The Kisan credit card introduced in India is a very innovative manner to support farmers and enable straight through processing.

However, carrying multiple cards for different purposes leads to inconvenience and days are not far off when a single card will be able to cater to multiple services similar to a mobile phone which has now converged other electronic devices such as music player, video and camera.

b. Type of Cards

Cards can be classified in different ways. The classification could be based on business usage like personal, corporate, etc. They can also be classified based on the technology used like magnetic stripe cards, smart cards with contact and contactless smart card. There can be overlaps between these classifications.

Credit Card

This is one of the oldest types of cards issued since 1950's. A credit card holder enjoys a credit limit that she can spend. These spends are billed in cycles and allows the card holder to have a revolving balance that one can pay off over a period of time.

There can be preset limits on the card beyond which the outstanding cannot increase.
There are cards that are issued to certain category of customers where there is no preset credit limit. These types of cards are generally issued to high net worth individuals who have very high limits. Theoretically the limit in these cards is unlimited.
In terms of popularity Credit cards are the most popular.

The new trend in the credit card segment is co-branded cards. For e.g., Jet Airways has tied up with MasterCard to issue a Jet airways Card where JP Miles can be earned on spend on this card. Yatra.com has launched a co-branded card with VISA.

VISA also launched theme cards such as Women's card / Students card etc.

Credit Cards can be further classified into various levels based on the credit score and spending patterns. Typically, the lowest card is the standard, followed by Gold and then Platinum. A new level is World Card. In addition to the limit differences in the card, the facilities provided as well as the charges applicable on the card vary.

Charge Cards

Very often one will come across the terms Credit card/Charge cards. Both these words are used interchangeably by the world at large.

There are conspicuous differences between a credit card and a charge card.

A charge card requires the card holder to repay the balance in full at the end of each billing cycle. A credit card on the other hand allows the card holder to have a revolving balance that one can pay off over a period of time.

Some cards do not have a preset credit limit giving one a limitless amount of credit.

There are certain restrictions on the transaction that can be undertaken on charge cards.

American Express and Diners Club Charge cards are the most popular.

American Express charge cards are again classified to cater to the different strata of the society and the Platinum charge card is the most sought after. The Platinum charge card is also a status symbol among the elite. Some cards are by invitation only and may offer many outlandish perks.

Debit Cards

Debit Cards are of recent origin. This card evolved after the technology evolution wherein the settlement was electronic. The cardholder can spend up to the amount which is available in the account of the customer. Excess use is treated as an account overdraft and carries associated charges. These cards are typically linked to the operative account of the customer and validation of the balances happens prior to the spending on the card.

These cards are credit risk free (to a certain extent) from the perspective of the issuer as the issuer does not carry the default risk at all. The element of risk may be there when a merchant transaction is affected without checking the balances in the card. In order to overcome this certain Issuers have come out with a variant of the Debit Card which can be 100% online; for E.g., VISA Electron. These cards can be refused in certain circumstances like non-availability of connectivity. Similarly the manual swipe cannot be used on the electronic cards

ATM Cards

ATM cards were used solely for the purpose of cash withdrawals. Initially, the ATM card could be used only in the network of the Card issuer itself, i.e., if X bank issues an ATM Card the Card could have been used only in the network of that bank and nowhere else. This reduced the utility value of the card and the customer had to carry a separate card for ATM and a separate card for Debit Card.

Even today, one may come across this type of card in certain technologically underdeveloped countries.

Credit card cum ATM Cards

Modern day credit cards offered by institutions also has the facility for the customers to withdraw cash. Separate cash limits are set on the credit card for the same. This takes care of emergency cash requirements of the customer.

However, cash withdrawal on credit cards entails service charges over and above the normal transactions.

Debit card cum ATM Cards

The ATM cards can also cater to the customer's need of using it as a Debit Card.

Unlike a Credit Cum ATM Card, the overall limit, be it cash withdrawal or using the card as a debit card, is restricted to the balance in the operative account to which the card is linked. In certain countries/issuers also call the debit card as Check card as it is as good as a check (in the Indian context cheque). The issuer may also offer overdrawing facility to a certain extent.

For example, VISA has two types of cards - VISA Debit Card and VISA Electron. VISA electron cards cannot be overdrawn as the balances are checked online. Some merchant establishments may not accept Electron Cards

Another major development in this segment is the interoperability between issuers within networks and using the cards on a common platform. Typically a customer who has a debit cum ATM card issued by an issuer bank issuing a VISA can use this card for withdrawal of the cash from any bank's ATM which is also a member of VISA. In the past if the Debit Cum ATM card was issued by Bank A, the customer had to necessarily go to the A Bank's ATM only for cash withdrawal while other merchant transaction could be done with any VISA affiliated merchant.

VISA is only an example; there are other issuers like MASTER. There are other shared payment networks. For e.g. in India we have a network called BANCS which caters to those ATM network for Banks which are not part of the VISA and MASTER. (Earlier there was a network called Swadhan).

The biggest advantage of using the Debit cum ATM cards of Global network organizations like VISA and MASTER is the same card can be used to withdraw cash not only in the local currency but also in foreign currency when the customer travels abroad; for e.g., when an Indian customer having a VISA card issued by a bank in India travels to Riyadh and sees an ATM of a Saudi Arabian Bank with VISA logo on the ATM, she can walk into the ATM and do cash withdrawal in SAR (Saudi Arabian Riyals). (The exchange rate and the services charges are the hidden cost in such a transaction which needs to be worked out vis-à-vis carrying a travel currency card).

Travel Currency card cum ATM Cards

This is a new type of cards. They are cards preloaded with a specific amount. It can be issued in multiple currencies. The same card can be used as an ATM Cards.

VISA and Master issue these types of cards.

In the Indian context, the difference between Debit cum ATM card and Travel Currency card are as follows:

- For a travel card, the exchange rate is locked in at the time of purchase and not across the period of spending
- If one is travelling to multiple countries, one may have to carry multiple travel currency cards for different currencies which become a bit cumbersome.

- A travel card issued in India strictly cannot be used in India (for withdrawing Rupees)

The travel currency card becomes handy to those people who do not have a debit card / bank account of the desired currency. Other facility in this card is that it can be topped up as required. Unused amount on these cards can be surrendered/refunded, if the unutilized amount is above a threshold level.

Gift Cards

The concept of Gifting has undergone a sea change in modern times. Gift vouchers are being replaced with Gift Cards universally.

Technically, both Gift Card and Travel currency cards are pre-paid cards. In case of the former the same cannot be topped up once the limit is exhausted while in case of the latter the same can be topped up. Moreover, gift cards are usually of the same currency in which they are bought.

Petro Cards

There are different variances of the Petro Cards.

The Petro Cards in India are stand-alone prepaid cards. Both BPCL and HPCL have come out with the Petro cards. However BPCL is the most popular petro card. The attraction towards this card is the loyalty bonus and other discounts.

The second variant of a petro card is the Co- Branded Petro Credit Card similar to the co-branded credit cards of Airlines. For e.g. in Canada there is Citi Petro Points Master Card.

The third variant of a Petro Card is linking the petro card to a Credit card. One such company which issues such a card is Petro Canada. The petro card of that company can be linked to the credit card for a consolidated view of the same

Corporate Cards

All the major card issuers have launched cards for business houses.

Businesses are typically classified into

- Small Business
- Mid-size
- Large companies
- Government and Public Sector

Unfortunately the definition of the first three business classification varies from issuer to issuer. For e.g. Master Card defines a Mid-size / Medium Sized business as one having revenue between USD 10 Mio and USD 1 Bio, while VISA's definition is one having revenue between USD 25 Mio and USD 500 Mio.

The business cards can be issued either to particular employees / individuals or to the organization. Certain cards can be assigned to specific departments within an organization. In case of individuals, these cards are generally issued to the middle and senior management for their travel and other expenses incurred like entertainment. These may also be issued to the procurement teams.

The basic purpose of issuing such cards is for the purpose of control and convenience.

Control from the perspective of spending limits, type of spending, legitimacy of spends, etc. The convenience factor is from the perspective of repayment in an effective and efficient manner. It also enables corporations to monitor the type of spending as well as patterns of spending.

Businesses are wooed by card issuers with a number of features on the card as well as other add on features.

The facilities to the corporate are innumerous. They have different types of cards .The business card need not necessarily be a credit card. It can also be a debit card or a prepaid card.

VISA has the following type of Business cards for small business

- VISA Business Credit Card
- VISA Business Debit Card
- VISA Business Line of credit
- VISA Signature Business Card
- VISA Gift Card
- VISA Incentive Card

For medium and large corporate the cards can be basically classified on the spend types viz. Corporate Travel Card, Corporate Purchasing Card, Corporate Fleet card. There are integrated cards that take care of all three functions (corporate travel card, corporate purchase card and corporate fleet card).

The differentiator for the business cards is the frills and additional resources etc. provided by the issuer.

In case of growing economy to exercise better control and monitoring the business card segment is poised for growth in the days to come.

Other Private Prepaid cards

The concept of prepaid cards are picking up in developing countries. In India the most popular prepaid cards which are of multipurpose is ItzCash. It can be used to transact on mobile as well as the internet. These cards can be used for making utility payments as well.

However the challenge for the private players compared to Master and Visa is the widespread acceptability of these cards.

Non-Financial Cards

The second segment of the cards which has sudden spurt in the recent times is the Non-financial type of cards.

The typical types of cards are

Frequent Flier cards issued by Airlines / Reward Cards

These cards are used for tracking the frequent flier miles accrued. These cards cannot be used for undertaking financial transactions.

Basically these cards are used for awarding mileage points based on different business logic.

There are grading in these cards as well. For e.g. Jet airways have JP Blue, Blue Plus, Silver, Gold and Platinum. Most of the big travel companies do offer such cards.

Airlines have gone beyond mileage points only for source airlines. There is code sharing arrangements between airlines wherein if one flies a partner airline, the passenger is available for Mileage points. For e.g. If one is a Jet Airways Frequent flier and flies

Malaysia airlines, the mileage points can be earned on the flights of Malaysia airlines. Over and above the code sharing with other partner Airlines, they have also tied up with other partners like Hotels.

The frequent flier cards are different from the co-branded credit cards issued.

Co-branded cards, as already mentioned above, are typically credit cards issued jointly which gives special facilities to the cardholders.

The new concept in the travel industry is the credit card point conversion programs. This is applicable to non-co-branded cards as well.

To illustrate, if a Citibank Platinum Card holder has 10000 reward points the same can be exchanged for JP Miles with jet airways. The conversion ratio varies from type of card. In case of a Platinum card 1 point on a credit card can be exchanged for 2.5 JP Miles

Loyalty cards issued by Hotels

This card is very similar to the frequent flier programs. The facilities offered on this card vary from hotel to hotel.

Some of the most popular programs are of

- Starwood Preferred Guest
- Marriot Rewards
- Hilton Honors
- Hyatt Gold Passport

Similar to the code sharing arrangement of airlines, the hotel programs also have a chain of hotels under their umbrella

Fuel Management Cards

In Canada the most popular Fuel management card is the Super Pass TM issued by PETRO CANADA. The business logic is a hybrid between individual cards and corporate cards. The cards can be issued to company drivers for refueling etc.

Lot of innovation has been built into this card in terms of control like which fuel station can be used for refuel, time of refuel, etc.

c. The Participants in the Card Business

The card industry has a number of participants in the processing. The role of each participant needs to be understood clearly before delving into the Card Dynamics.

The major participants in this market can be classified as follows:

Sr No	Participant Name	Participant Role
1.	Global Technology Companies	Visa, Master and Discover are examples of such companies. These companies per se do not issue cards, extend credit or set rate and fees for consumers
2.	Card Issuers	An Institution which issues the card is referred to as the card issuer. Generally, banks are the issuers. It is the issuer that extends credit and sets rates and fees for consumers.
3.	Acquirer	An organization that collects (acquires) credit authorization requests from Card Accepters and provides guarantees of payment. The acquirer can also be a financial institution.
4.	Issuer Cum Acquirer	American Express cards and Discover are examples of Issuer cum Acquirer

5.	Merchant or acceptor	An individual, organization, or corporation that accepts credit cards as payment for merchandise or services
6.	Card Holder	Last but not the least the most Important participant in the Card business is the card holder who uses cards for making transactions.

d. Private Label and White Label Cards

In addition to the various classifications on the end use of the card, cards can also be classified as private label cards and white label cards. This classification is over and above the normal cards (there is no default name for the normal cards).

Private label cards can be used only at the merchants own network. The BPCL petro card for example is a private label card as the Petro card cannot be used anywhere.

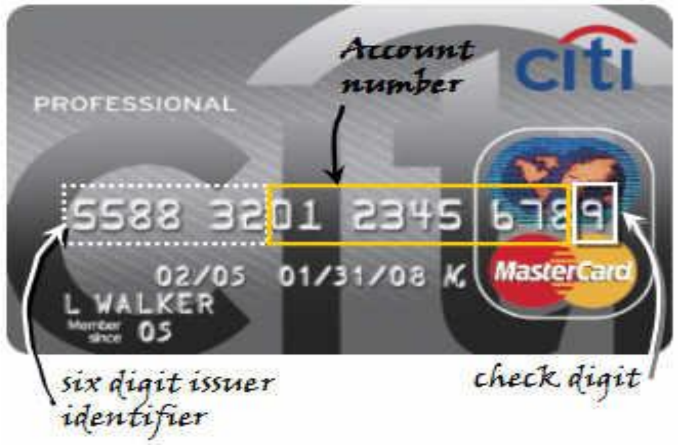
White Label Card on the other hand is launched by a merchant in association with the issuer and the VISA/Master card. However it will not hold the name of the issuer. The same can be used freely like a normal credit card. For e.g. Reliance Capital can tie up with State Bank of India for a white label Visa Card. When such a card is issued, it will carry only the name of Reliance Capital and the name of State Bank of India will not feature anywhere on the card. This is basically done for the revenue sharing purpose

e. Understanding the Card

The credit card has a number of attributes on the card. (Discussed below are the attributes of credit card only and not other cards) Some of them are visible to the naked eye while some others are not.

The attributes are categorized based on the front side of the card and the back side of the card.

Front side card attributes



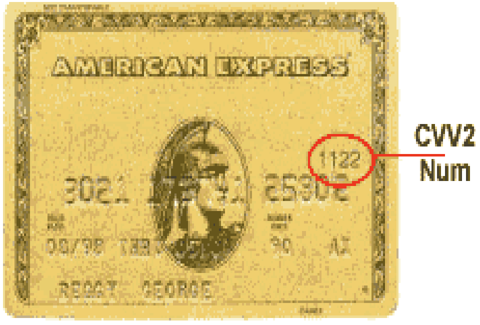
The key attributes are

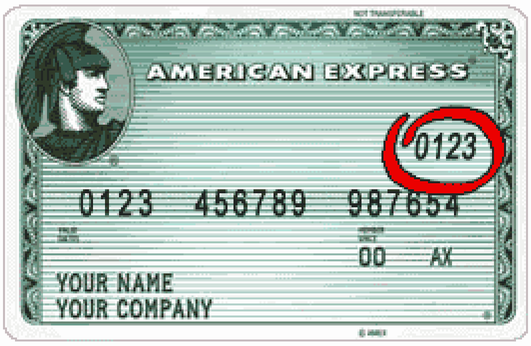
- The Card issuer in this e.g. Citi Bank is the card issuer
- The card is a Master Card
- The card type is Professional
- The card number (more of it later)
- The issue date in MM/YY format
- Valid through Date in MM/YY format
- Name of the card holder
- Additional information in this card mentioned above is the age of the relationship of the card holder with the issuer
- For smart cards, the chip is also present in the front of the card

In case of credit cards the card number, the issue date, valid through date and the card holder name is embossed (creating raised letters and numbers on the cards). In the early stages of evolution of the credit card and before the advent of electronic POS (Point of Sale) Terminal, the charge slips were manual. The embossing would help imprinting i.e.

using the embossed information to make an impression on the charge slip. This was to increase efficiency at the same time to prevent frauds on charge slip.

In case of American express credit cards, the Card Verification Value 2 (CVV2) is also in the front of the cards while in other cases it is at the back of the card. (CVV2 will be discussed when the back side of the card is discussed.) The CVV2 in these cards are not embossed





Card Size

One may be wondering why the card size for all different types of card is very similar. There are specific ISO Standards for the card industry. Standardization is important for interoperability of various acquirer devices on different cards (ATM slots, Merchant POS devices, Manual card machines, etc.). There are series of standards which the card industries follow

The ISO Standard **ISO/IEC 7810:2003** specifies the following:

- The cards have to meet a nominal thickness
- Four different sizes of cards of which ID-1 85.60mm x 53.98 mm is used for ATM, credit and Debit Cards
- The construction and materials of the identification cards
- The physical characteristics of the card such as bending stiffness, flammability, bending thickness, toxicity, resistance to chemicals etc.

Card Numbering

The card numbering also has been standardized and the ISO Standard relevant to Card numbering is **ISO/IEC 7812-1:2006.**

The card number can be split into 4 components:

1- Major industry Identifier (MII)

2-Issuer Identifier –the first six digits including the MII

3-Account identifier

4- Check Digit

A card can have a maximum length of 19 digits

MII-Major Industry Identifier

This classifies the entity which issues the card

MII Digit Value	**Issuer Category**
0	ISO/TC 68 and other industry assignments
1	Airlines
2	Airlines and other industry assignments
3	Travel and entertainment
4	Banking and financial
5	Banking and financial
6	Merchandizing and banking
7	Petroleum
8	Telecommunications and other industry assignments
9	National assignment

It is interesting to note that American Express Diners Club and Carte Blanch are in the travel and entertainment category.

Issuer Identifier

The issuer identifier is depicted in the table below:

Issuer	**Identifier**	**Card Number Length**
Diner's Club/Carte Blanche	300xxx-305xxx, 36xxxx, 38xxxx	14
American Express	34xxxx, 37xxxx	15
VISA	4xxxxx	13, 16
MasterCard	51xxxx-55xxxx	16
Discover	6011xx	16

Account Number

The seventh digit to the penultimate digit on the card is the account number of the client. As the maximum card number can be 19 the account number field can vary between 6 digits to 12 digits.

Check Digit

The last digit on the card is the check digit. The check digit is arrived using an algorithm called Mod 10 or Modulus of 10.This algorithm is popularly known as Luhn algorithm, after IBM scientist Hans Peter Luhn (1896-1964), who was awarded US Patent 2950048 ("Computer for Verifying Numbers") for the technique in 1960.

There are multiple ways to check whether the Credit card number is valid or not based on the check digit.

The same is explained using an example. The example given below is not to arrive at the check digit, but to check whether the card number provided along with the check digit is valid card number or an invalid card number.

Step1- Write the numbers in the reverse order

Step 2- Double the even digits of the result of step 1

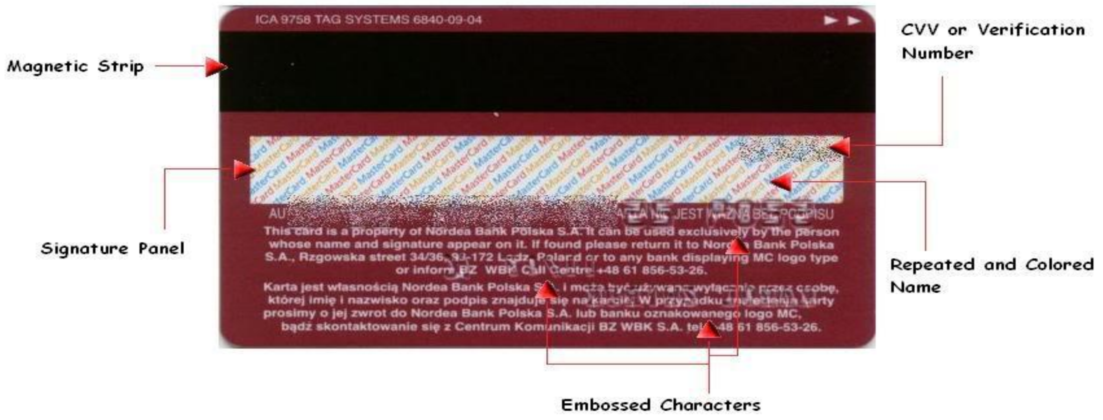
Step 3-In case any of the results of step 2 is having more than one digit add up both the digits

Step 4-Sum up all the results of Step 3 as well as the odd digits as it is. If the final sum is divisible by 10 then the card number is valid

Card Number	4	3	3	9	5	0	1	2	2	9	4	8	4	5	5	6
Step 1	6	5	5	4	8	4	9	2	2	1	0	5	9	3	3	4
Step 2		**10**		8		8		4		2		**10**		6		8
Step 3	6	1	5	8	8	8	9	4	2	2	0	1	9	6	3	8
Step 3	6+1+5+8+8+8+9+4+2+2+0+1+9+6+3+8=80.80 is divisible by 10															

The objective of a check digit is to prevent erroneous keying in of numbers as the check sum can identify single transposition and wrong keying in of data. This is not a security feature to prevent malicious attacks.

Back side card attributes



The key attributes of the back side of the card are

- Magnetic strip (more of it later)
- Signature Panel
- CVV or Verification Number(more of it later)
- Other terms and conditions/Contact numbers(which one rarely reads)

Magnetic Strips

The ISO/IEC 7811 series and ISO/IEC 7813 lays down the specification related to embossing and magnetic strips, their contents etc.

The standards have gone to the extent of mentioning the position in terms of distance from the beginning of the card, the position of each value as well.

In a magnetic stripe there are three tracks.

Track1 - Used to store the basic card information. Within Track1 there are multiple formats. The Formats used by banks is Format B.

It has a higher bit density of 210 bits per inch (bpi) which can accommodate 79 7-bit characters.

Track2 - This track was specifically developed by the American Bank Association for financial transaction.
It has 75 bits per inch (bpi) which can accommodate 40 5-bit numeric characters

Track3 - This is also used for financial transactions. **However as on date nobody is using the same in the debit and credit cards.** This typically can be used for prepaid cards.

The difference is its read write ability.
It has 210 bits per inch (bpi) which can accommodate up to 107 numeric digits.

There are certain redundant fields between Track1 and Track2 which is intentional. In the event that track1 is not readable by any chance the data can be read from track 2 and vice versa.

Track 1 and 2 data is standardized and details of each column are available in the public domain.

Magnetic strips also can be classified based on High Coercivity (HiCo) or Low Coercivity (LoCo). The former are harder to erase while the latter require low amount of magnetic energy to record.
The key attributes which are stored in the Magnetic stripe are

- Service Code in Track 2.The third digit in the service determines the card nature ATM/Cash or Non ATM/Cash as well as PIN required or not.

- Discretionary Data on both the tracks which may contain the Pin Verification Key Indicator (PVKI- 1 character), PIN verification Value (PVV, 4 Characters), Card Verification Value (CVV1) or Card Verification Code (CVC1, 3 characters). These values are calculated based on the card attributes and then encrypted. This is also known as Card Verification Key (CVK).

CVV 2

This is one of the most important values on the back side of the card. This information is not stored in the magnetic strip, to prevent frauds. A CVV2 is typically used for ‘not in person transaction’ like an internet or a telephonic transaction.

There are certain guidelines on storage of CVV2 by Merchants. (The same will be covered in PCI-DSS section)

Chip Card

The magnetic stripe card had some inherent security risks like Card Skimming .Skimming is the most popular form of identity theft in the credit card industry. In a skimming mechanism the magnetic strip of the card is duplicated at the time of swiping the card by some external devices. This external device captures the full details on the magnetic tracks and is subsequently used to create duplicate cards. The advancement of technology also brought in innovative ways of mitigating this risk.

The latest product now available is the Chip Card. A chip card is typically a smart card which has a microprocessor embedded in the card which replaces the traditional magnetic strips.

ISO/IEC 7816 series deals in the details of the Chip.

One of the biggest challenges is the migration of the existing cards into the chip cards. More critical than the card replacement is the replacement of card readers (POS Terminals)). Similarly, the ATM Machines also use the magnetic stripe. Both of these pose a bigger challenge.

VISA has issued deadlines in Canada as 1st October 2010 for migrating to chip cards. In the events the merchants do not move to this technology, the fraud liability will no longer be borne by VISA.

The Chip card also comes with a PIN which replaces the traditional signature of the card holder.

Another interesting challenge is what happens to an international card holder of Canada travels to India or any other country where there is no mandate for chip card? This necessitates the need of having a Hybrid card, i.e., Chip and Magnetic Stripes. Chip and PIN Visa Canada currently issue hybrid cards.

2. Card Issuance

There are two key attributes pertaining to card issuance:

- Client identification and profiling
- Client's credit risk profile specifically for credit cards

a. Client identification and profiling

It has become absolutely mandatory for card issuers to identify the credentials of the constituent. This is also part of the Know Your Customer (KYC) process. There are various regulations across different countries to establish the identity before the card is issued. This applies across the services industry segments. To get a SIM card too, identification is a must.

There are two dimensions to identification. The first is identity of the constituent per se and the second is address proof to ensure that the constituent resides at an identifiable place.

There are certain documents that fulfill both dimensions such as driving license, while in other cases there are two separate documents to establish both dimensions separately.

The Patriot Act of USA is also applicable to the credit card industry. The constituent (applicant) will have to fill up a standard application form of the card issuer, which will cover the basic demographic information of the constituent.

In case of debit cum ATM cards, client profiling will form a part of the account opening process and there is no need for a separate process.

There is a new concept of Insta Kits (instant cards) by certain banks, where a customer is given an account number and a debit card across the counter. In such cases, the debit card will not be personalized i.e., the card will not carry the card holder name. This type of card is also used in case of 'card lost / damaged' situations till the new card is being created.

b. Client credit risk profile

This is one of the key inputs for arriving at credit limits, which are granted to the constituent. The ability to pay back the outstanding amount depends on a number of factors including regular income, spending on the card, mortgage and other loans, etc.

Often a constituent may have a number of liabilities, mortgages etc. The same may not be revealed by the constituent as a part of the application process. This can lead to huge credit risk for the card issuer.

This problem is obviated through an independent credit bureau. The role of a credit bureau in any country is to aggregate the credit history of constituents and any organizations proposing to lend to the constituents will approach the credit bureau with regard to the standing of the constituent.

The top three credit bureaus in the US are Experian, Transunion and Equifax. In the Indian context, CIBIL (Credit Information Bureau of India Limited) is the first credit Bureau. Experian has recently started its operation in India as well.

Each constituent is given a score by the credit bureaus. The most popular credit score used by the top three credit bureaus is FICO. This score software is attributed to **F**air **I**saac **Co**mpany.

The card issuers independently verify the FICO score provided by the credit bureaus before fixing the limits.

One has to be very careful when undertaking a financial liability transaction, as the FICO score is a dynamic one and keeps changing. It is interesting to note that by closing an existing credit card, one's FICO score drops.

c. Card generation and printing process

The card generation and printing process is managed electronically. A number of softwares are available in the market for the entire card management life cycle.

Once the card has been approved, the card needs to be printed/embossed. This is a two-step process. Generally, the logo, color and front and back as well as all other static data are printed in the first round.

In the second round of printing/embossing, customization happens. At this stage, the magnetic stripe is also coded with necessary data. Chips are configured in this stage.

Generally, the entire process of printing is outsourced to specialist printers.

However, the necessary security controls need to be ensured as the issuer may be parting with the card holder data. Requirement 12.8 of the PCI DSS Ver 1.2.1 has laid down the controls related to the service providers.

There may be standard SLAs (Service Level Agreements) for each service delivered by the service provider.

The cards have to be dispatched to the customer directly by the card issuer or on behalf of the issuer by the service provider. To ensure that the card is not delivered to the wrong person, courier agencies are specifically instructed to ensure that they also cross check some identity document before handing over the same to the constituent. The address is also verified by some means in the ‘Identification’ phase for the accurate delivery of card, pin, statements, other materials, etc.

d. PIN generation and printing process

The PIN generation processes can also be a core functionality of the card management software.

There are generally three types of PIN. One is card Pin for ATM /POS Terminals, the second is T-Pin or the Telephone Pin, and the last is the Internet Pin. The Internet Pin can again be sub-classified as Q Pin (Query) and H-Pin (Transaction).

In some systems, the ATM Pin and T-Pin are generated together. Some software does not support T-Pin for which separate software needs to be in place for Tele Card Transaction Processing.

The Q-Pin and the H-Pin are generated by the card holder and there is no need for dispatch of those Pins. These may be passwords or one-time codes generated using secured devices.

Controls on dispatch of Card and Pin are necessary to prevent fraud. Normally, as a best practice, the same will be dispatched by two separate courier agencies. Similarly, if the Pin is not used for the first time or three months have elapsed from the last transaction, the Pin needs to be changed or the account is disabled.

e. Handling returned cards

Strong controls are required for this process as there is a huge risk of misuse. All returned cards have to be kept in dual custody.

There should be a process to record all returned cards at the card issuer’s end. Similarly, all returned cards retained for more than a specific period (say six months) need to be destroyed with proper authorizations.

In case of returned cards, at least three attempts must be made telephonically to contact the customer and necessary attempts have to be made to deliver the card.

f. Primary Cards and Add on Cards

The principal card is issued to the primary credit card applicant. To entice the customer and boost usage, the card issuing companies have come out with a new feature called add-on cards.

Add-on cards are generally issued to spouses, children and other close relatives. There is no independent limit on these cards. However, the limit of credit available in case of multiple cards will be within the overall limit given to the primary card holder.

In case of Debit cum ATM cards issues on joint accounts, cards can be issued to all the account holders. The first name in the account will be the primary account and the other holders will be treated as add-on.

In case one customer is holding more than one bank account in the same bank in different combinations, it is possible to link a single card to multiple accounts.

For e.g., A & B has an account Acc1 and B & A has account Acc2 in the same bank, A will be issued a single Debit cum ATM Card which will be linked to Acc1 as well as Acc2. There are certain complications in this which can vary from ATM to ATM and country to country. In certain ATMs/countries, it will prompt the user to decide the account from which he would like to withdraw cash. In others, there is no such provision and the primary account from which the card is issued is debited by default.

g. Balance Transfer from one card to another

In the days of the hot competition, the dirty face of the card industry was balance transfer from one card issuer to another card issuer to reduce the outgo of the cardholder.

This is akin to the subprime story where customers were moving the mortgage loan from one organization to another organization. There is 0%Balance Transfer Credit Cards in US. One might be wondering as to the reason for issuing such credit card and what the issuing company gains. If one reads the fine print this 0% will be valid for a specific period say for first 6 months or first 12 months of transfer after which it will attract the normal service charges. Process wise it is very simple.

h. Terms and Conditions of credit card issuance

One of the most ignored aspects of requests for a card is understanding the card terms and conditions. We almost blindly resign to fate by signing account opening documents. Finally, when there is a dispute the card issuer will use the Terms and Conditions Sheet signed by the constituent.

Cards in the US are not issued to people under the age of 18.

Generally the T&C (Terms and conditions) are printed in such small font that one can rarely read it. The items are also huge. In the Indian Context RBI has come out with one more concept of Most Important Terms and Conditions, which is an extract of the Terms and Conditions. The constituent is expected to at least know the most important terms and conditions.

The Most Important (MITC) or the Key Terms and conditions of a credit card as per RBI Master circular (This can be construed to be applicable globally as well) are given below. RBI has gone to the extent of mentioning the Font size of the MITC to be minimum Arial 12, if not bigger.

i. Fees and Charges

- Joining Fees for Primary Card Holder and for add-on card holders
- Annual Membership Fees for Primary Card Holder and for add-on card holders
- Cash Advance Fee
- Service Charges Levied for transactions
- Interest Free(Grace period)-illustrated with examples
- Finance Charges for both revolving credit and cash advances
- Overdue Interest charges-to be given on monthly and annualized basis. In the US market the interest charges are quoted in APR (Annualized Percentage Rate).There can be multiple APRs ,one for Purchases, the other for Balance Transfer and the third for cash advances and convenience checks
- Charges in case of default

ii. Drawing Limits

- Credit Limit
- Available Credit Limit
- Cash Withdrawal Limit

iii. Billing

Billing statements—periodicity and mode of sending

- Minimum amount payable

- Method of payment
- Billing disputes resolution
- Contact particulars of 24 hour call centers of card issuer
- Grievances redressal escalation—contact particulars of officers to be contacted
- Complete postal address of card issuing bank
- Toll free number for customer care services

iv. Default and circumstances

- Procedure including notice period for reporting a card holder as defaulter Procedure for withdrawal of default report and the period within which the default report would be withdrawn after settlement of dues
- Recovery procedure in case of default
- Recovery of dues in case of death/ permanent in capacitance of cardholder
- Available insurance cover for card holder and date of activation of policy

v. Termination / revocation of card membership

- Procedure for surrender of card by card holder - due notice

vi. Loss/theft/misuse of card

- Procedure to be followed in case of loss/ theft/ misuse of card-mode of intimation to card issuer
- Liability of card holder in case of (i) above

vii. Disclosure

i) Type of information relating to card holder to be disclosed with and without approval of card holder.

The disclosures will happen in various stages and RBI has identified four stages in which the disclosures have been made:

- During Marketing
- At application
- At welcome kit
- On billing
- On an on-going basis, any change of the terms and conditions.

3. Card Maintenance

a. Demographic Details

In the US, social security number (SSN) is required to open a bank account or have a credit card. The equivalent of SSN in India is PAN. There are three types of social security numbers allotted in the US. (Please visit www.ssa.gov/pubs/10002.html for further details.) This identifier seldom changes.

An SSN or Tax Identification Number becomes a critical control for issuance of cards.

In many situations, a credit card holder data keeps changing. Typical demographic data includes:

- Address details
- Telephone number land line and hand phone
- Email addresses

Regulations are becoming stricter and these changes cannot be effected without sufficient documentary proof. Every demographic change must be supported by documentary evidence.

Other demographic details that do not change are:

- Date of birth of the card holder
- The sex of the card holder
- Mother's maiden name

Many times, demographic details are used for identification of the cardholder over telephonic or Internet channels.

Sometimes a hint question, such as "What is your pet's name", are also captured as a part of the Internet channel for identification.

Some forward looking companies also collect personal details such as spouse's and children's names. The objective of collecting this information is cross selling.

The second set of client information requested is related to financial status.

This is critical information, which is required for arriving at the credit worthiness of the constituent and eligibility for credit limit. This information is sought mostly for credit cards.

b. Card upgrades

Many times, a customer may opt for standard cards. Over a period of time, based on the card spending patterns and credit history of the card holder, cards are upgraded periodically. The card issuer may define some internal business rules and periodicity to review the existing cards. If the card issuer is satisfied with the transactions on the card, the cards can be upgraded. The cardholder may request for the upgrade herself.

A normal upgrade is in stages starting from standard, silver, gold, and platinum and now a new upgrade classification is World Card. The business rules of the card issuer can also comprise a minimum period for holding each type of card; for e.g., for a person to be upgraded from Gold to Platinum, the Gold card should run for 12 months.

One of the most important points to be noted in case of upgrade is that the card numbers will keep changing at every upgrade. Hence, in the month of transition, the customer may receive two statements, one for the non-upgraded card and one for the upgraded one. However, the balance transfer and the outstanding and loyalty points, if any, will be carried forward.

For frequent flier cards, the business rules for upgrade would be x number of miles and / or number of flights. The business logic for a non-finance card can be very complex and can be based on a wide number of parameters.

The upgrades can be a part of special promotion. The same can be induced by the card holder or at the discretion of the card issuer.

c. Add-on cards issuance

The process of issuance of an add-on card is similar to the issuance of the primary card. The add-on card applicant will also have to fill up the requisite form. The details of the add-on card holder also need to be furnished including the demographic details.

This is managed by the card management software. The key difference in the process is that the add-on card has to be linked to the primary card for credit limit control.

d. Unsolicited Cards

Many times, a card issuer may issue unsolicited cards to the existing card holders. In such cases, the original card application will be treated as the source document. There are restrictions on issuance of unsolicited cards in certain countries. In India, RBI restricts issue of unsolicited cards.

In the US, in 1958, more than 60,000 unsolicited cards were issued by Bank of America (BoA) as a part of marketing strategy. The same was outlawed in 1970, but not before 100 million cards were issued.

e. Hot listing of cards

I. Based on customer request

The card holder may lose the card accidentally or it may be stolen. To prevent misuse of the lost/stolen card, the card holder needs to urgently report to the card issuer. Earlier, reporting of a lost card was cumbersome. With the evolution of different channels such as telephone and the Internet, the entire process has undergone massive changes. Now, most of the card issuers take such hot listing requests over telephone, which has become the most popular channel for receipt of such requests. This is because it is most easily accessible. This also reduces the time between loss of the card and reporting of the incidence. The liability of the cardholder in case of spends on a lost / stolen card is restricted to a certain limit ($50 in the US).

II. New card in lieu of hot listed card

Hot listing the card is only one part of the process. In most occasions, when the hot listing has been done at the instance of the card holder, a fresh card needs to be issued to the card holder.

The fresh card will bear a new number. However, the documentation such as SSN is generally not taken again.

Many times, an existing card can be hot listed by the card issuer and a fresh card can be issued. One of the reasons for this could be card issuer's policy based on the probability of fraud. One such example of a card issuer is Citibank. In case of international cards, a couple of years ago, if the card holder used the card in the South East Asia, specifically Thailand, Hong Kong and Singapore, Citibank would issue a fresh card to the card holder. The type of credit card fraud which was most popular in that region was card skimming (more of it in the Fraud Section). Citibank thought that the probability of the compromise of the card was high. As a result, all those cards which were swiped in these countries were replaced by Citibank.

In some instances, issuers issue temporary un-personalized cards for instant use till the new plastic card is created. These cards are valid till the replacement card is ready for use / a fixed time has elapsed, whichever comes first.

III. Based on delinquency

The card issuer regularly monitors the track record of the card in terms of payment status and the outstanding. The card issuer can have internal business rules to define delinquency, and based on these rules the card will be hot listed.

If the card is hot listed, the cardholder will continue to hold the card but will not be able to use the card either at the merchant establishments or at ATMs.

IV. Inactive cards

Many cards become inactive over a period of time. There could be multiple reasons a card holder may not be able to use a card. Such inactive cards are also susceptible to frauds. The card issuer can define the business rules for defining a card as an inactive card. The business rules could be no merchant transactions or cash withdrawals.

It is necessary to segregate customer-induced transactions and issuer-induced transactions which include debit for charges, interest, card fees etc.

One dimension of defining the same as inactive could be the period for which no transactions happen. It is mandatory to identify transactions that need to be skipped to arrive at the period of inactivity. One such example would be issuer-induced transactions. Based on this logic, the cards would be hot listed and the card holders would not be able to transact on these cards.

Some cards are returned undelivered for multifarious reasons. These cards also need to be hot listed. They need to be physically destroyed as well.

i. Swallowed Cards Management

In many ATMs, there is business logic of cards being swallowed by the ATM in case the ATM PIN has been entered wrongly by the card holder a certain number of times. This happens in case of both credit and debit cards.

There are two approaches to handling swallowed cards if the card is swallowed by the card issuer’s ATM itself. These are centralized and decentralized approaches. In a centralized approach, the card is dispatched to centralized operations, which in turn will send it to the card holder. In case of a decentralized approach, the card is sent by the ATM department to the card holder.

On many occasions, the card may be swallowed by a third-party ATM. For e.g., a VISA card issued by Citibank; the card holder tries to withdraw from the HSBC VISA ATM. In this case, the card swallowed by HSBC ATM will be sent to Citibank.

Swallowing of cards is a good feature to control frauds. However, all ATMs are not equipped with the card swallowing mechanism. Dispatch of cards back to the card holder is a long-drawn process. There are detailed guidelines issued by Visa as to how such cards needs to be handled. The reader may refer to Visa-international operating regulations.

ii. Card Recovery Procedure By merchants

A merchant, during the course of business, may encounter the following situations:

- A counterfeit card
- A hot listed card
- A card left inadvertently by a customer after swiping it at the merchant's establishment.

In all cases, the merchant must report and return the card to the issuer within maximum five days of such instances.

In case of non-chip cards, they should be cut horizontally to prevent damage to the magnetic stripe, hologram, or embossed or printed account number.

In case of chip cards, punch a hole through the middle of the magnetic stripe to make it unreadable and cut away the corner of the card at the opposite end from the chip.

f. Issue of Duplicate Cards

A card holder might have a broken / damaged card. Many times, due to wear and tear, the magnetic stripes become unreadable. Under these circumstances, the card issuer will issue a duplicate card to the card holder. The duplicate card will be an exact replica of the existing card including the Magnetic stripe details as well as CVV2.

g. Reissue of Expired Cards

All debit and credit cards have an expiry period. The expiry period can vary across card issuers. Generally, it is 3 years or 5 years for credit cards and longer for debit cards. The card issuer will send the renewed card a couple of months in advance in case credit history has been good. No fresh documentation is required from the cardholder for issuance of a renewed card; the first set of documentation will be re-used. The following points are to be noted in case of expired cards:

- The card number remains **unchanged.**
- The valid from and valid through date **changes.**
- The magnetic stripe data also will change as the valid from and to details are part of key information used in the magnetic stripe.
- The CVV2 will also be **different** since it also uses the valid from and valid through values in the algorithm of arriving at CVV2
- The ATM PIN remains **unchanged.**

h. Insurance on card

Insurance on a card has a vast meaning and it needs to be understood as it is often confusing. Insurance related to a card can be broadly classified as:

- **Zero Lost Card Liability** to the card holder in case of lost card: this is nothing but insurance the card issuer takes on behalf of the card holder to compensate the card holder. However liability is limited to 24 hours prior to the time of reporting and for future liability only.

- Here also one has to read the fine print. Typically, cash transactions done at ATMs are not covered as the PIN cannot be compromised easily.
- **Card Protection Plan (CPP):** Many card issuers have come out with novel way to protect the card holder's interests. However, this scheme has received lot of criticism from card holders and a number of law suits have been filed in the US and the UK courts (will be dealt with in more detail later).
- **Travel Accident Insurance** benefits to the card holder. In this, the card holder does not pay any premium separately. In India, banks have now also come out bank accounts linked with accidental insurance (will be dealt with in more detail later).
- **Personal Accident Insurance**, wherein the card holder is debited insurance premium monthly for various types of insurance.

Basically, all these are general Insurance products clubbed with the credit card.

Card Protection Plan

Typically a card protection plan can have different variants:

HSBC has a Card Protection Plan (CPP) in India. The key features are:

- A free call to block all cards, not necessarily cards issued by HSBC. The customer service team of HSBC will contact the respective card issuers to get the card cancelled. HSBC must however have details of the cards he individual holds.

It can also take care of:

- Loss of other documents such as Passport, Tickets etc.

- Emergency travel and hotel assistance, domestic and abroad
- Fraud Protection Pre-notification and post-notification. (In case of pre-notification the liability is limited to seven days prior to the date of reporting)

This comes at a very nominal fee payable yearly.

The Citi Bank has a Card Protection Plan (CPP) in the US, which is quite different from the HSBC scheme in India. As per this plan, the card issuer promises to make minimum monthly payment on the credit card balance for one year if the card holder experiences certain “life changing” events, such as disability, loss of income, or marriage. The charges can be anywhere between 89 cents to $ 5 per $100 outstanding in the credit card balance. In case any “life changing” events happen, the card holder need not pay back for one year. However, there are a number of disqualifications (“conditions apply”, in the Indian context).

There has been a class action suit against Citibank recently in Pennsylvania. There was a suit in Florida against Capital One Financial Corporation, which was settled with undisclosed terms. Discover Financial Services is also fighting another payment protection lawsuit in New Jersey. All these litigations points to hiding of basic riders of the product to the customer.

This Card protection plan should not be confused with the purchase protection plan, also known as **Retail Purchase protection plan**. In this plan, purchases made under a specific type of a card are protected from theft and accidental damage for up to 90 days from date of purchase. Coverage is at two levels: per incident level and per card member account per year.

Travel Accident Insurance on Credit Card

Documentation is critical for claiming the accident amount. A key process in this is the nomination form a card holder has to fill.

The amount of accidental insurance is astronomical .For e.g., HSBC has an air accident insurance of Rs 1 crore. Beware. Although this could tempt one to rush to HSBC for a premier card, there are two fine prints for availing this:

- Fine print 1:The air ticket has to be purchased by a credit card
- Fine print 2: The card has been utilized for at least five transactions within the last 89 days of the date of the accident.

The notice of death has to be provided by the nominee to the designated insurance company (as the card issuer is only the facilitator).

Personal Accident Insurance on Credit Card

It depends on the innovation of the card issuer to come out with novel products. There are different insurance products linked to the credit card.

Basically there are two types of personal accident insurance. One is to cover the card outstanding liability in the event of death or permanent disability. The second one is to cover the card holder. The card holder’s nominee will receive the amount over and above the card liability. There will be two separate premiums that will be levied on a monthly basis for both these benefits. The card issuer may levy additional service charges for the same. The card issuer can define the various eligibility criteria and business rules for the same.

i. Standing Instructions on Credit Card

The reader must not confuse this with the standing instructions given by the card holder to the insurance company for regular payments. All the accident insurance mentioned above are insurance products packaged with the credit card. The standing instruction for payment of insurance premium is similar to the standing instructions for payment of utility bills like mobile payments.

j. Resetting/Reissuance of PIN

As mentioned in the earlier sections, PINs are classified into ATM, Internet (QPin), HPIN and T-Pin. Generally in the case of compromise of the ATM/POS PIN, the same will be sent by mail to the cardholder's address at the specific request of the card holder.

In case of T-Pin, the same can be reset on the telephonic channel after due identification of the card holder. The Internet PIN can be reset by the card holder himself. Since last year, in many countries, all Internet transactions require the CVV2 as well as the Internet PIN. The Internet PIN is branded by VISA as Verified by VISA and SecurCode by MasterCard. The process for resetting the Internet password or obtaining an Internet PIN has been simplified by VISA. In case of ATM /Credit Card that are inactive, the ATM PIN also will be reset and a fresh PIN will be issued on the request of the customer.

k. Credit Limit Enhancement

Credit card limit can be enhanced on a credit card at the request of the card holder or by the card issuer. In case of the latter, it is also known as unsolicited credit enhancements. The current FICO score is looked at for approving an enhancement.

Enhancements at customer's request

The customer will have to request for an enhancement on the standard format of the card issuer. The form can be filled in hard copy or filled up online. In certain cases, it also can be done telephonically. The card issuer will go into the merits of the case and after due approvals enhance the credit limit of the card. There are other business rules like the card must be open for minimum period of six months before an enhancement request can be entertained.

Each card issuer may have certain specific limits set for each type of card. For e.g., Citibank may take a policy decision that Standard and VISA cards have a maximum of USD 30,000/- and Gold Card has a maximum limits of USD 50,000.

So, if a standard card holder applies to enhance his limits to 35,000, this request will not be acceded to directly. In such a case, the existing card will be upgraded to Gold Card. However, the fine print will be the difference in the card charges between the standard card and the new gold card.

An important factor for the issuer to increase the limit is the credit rating of the card holder.

The following actions on the part of the card holder will increase his credit rating from the card issuer perspective.

- One should not spend more than the limit set by the issuer.
- One should use the credit card regularly.
- One should pay off the bill in full instead of revolving credit.
- One should avoid late payment.

Over and above this, the issuer looks at the current FICO score (already discussed in section 2).

Unsolicited Credit Limit Enhancements

Card issuers have been increasing credit limit in case of credit card and allowing overdrafts without notification in case of debit cards without the customers’ request. This would induce spending and would lead to a debt trap. Lot of heat is being generated on this topic in the US as well as the UK on whether such action is healthy for the system. Such unsolicited limit increase induces the card holder to spend beyond his/her means.

l. Card Closure

The card holder may no longer need a card of one issuer and would like to close the card. Normally, a request is received from the card holder. The card issuer, if satisfied with the health of the account, can close the card. The process will be similar to hot listing.

4. Merchant

A merchant or an acceptor is one of the key players in the card landscape. It is this merchant which is responsible for the popularity of a specific card. Merchants perform the role of a distributor in the product selling life cycle. The popularity of a card is known by the number of merchants linked to the Global Technology companies (i.e. network associations – visa, mastercard, etc.)

For e.g., Visa boasts of more than 30 million establishments worldwide and about 110,000 Merchant Partners in India and Nepal.

a. Merchant Category

Merchant establishments can be broadly classified into two categories viz. merchandising and service industries. Merchandising includes both stores and online sites. The service industry includes the Hotel, Travel, Food and beverage, Telephone Service providers, Internet service providers etc.

Many card Websites have now come out with spending patterns of card holders. This is basically done by categorizing merchants based on industry classification, which is a four-digit numeric code. Most issuers use this common code. Some popular category codes are:

Merchant Category Code	Merchant Category Description	Remarks /Example
4121	Taxicabs and Limousines	Meru Cabs
5812	Eating Places and Restaurants	Hotels etc.
5813	Drinking Places (Bars and Taverns)	Only Pubs which serve only liquor
5814	Fast Food Restaurants	McDonalds, Dominos, Pizza Hut
7230	Beauty and Barber Shops	Javed Habib
7298	Health and Beauty Spas	

A merchant can be affiliated to one or all the card payment providers.

There is no restriction for a merchant to be affiliated only to Master or Visa or Discover or any other card.

b. Merchant Classification

Different service providers can have different classifications based on their own internal guidelines. Visa has classified Merchants into three categories:

- Direct Merchants
- IPSP(Internet Payment Service Provider)
- Sponsored merchants

Master has classified merchants as

- Direct
- Payment Facilitators
- Sub-Merchant

Direct Merchants are institutions directly registered with Visa and enter into a formal and legally binding agreement with the acquirer.

Note: This document will follow the flow of Visa in terms of details. MasterCard follows similar framework, except for the parlance used. An understanding of one can lead to understanding of the industry as a whole.

c. Obligations of (Internet Payment Service Provider) IPSP

With the Internet catching up, this could be one of the growing businesses for an acquirer. An IPSP is typically a company that enters into an agreement with the acquirer and is approved by Visa to process and settle transactions on behalf of online merchants; E.g. Ccbill.com and epoch.com.

The IPSP in turn will enroll merchants to avail of the services. These merchants are not directly registered with the acquirer. They do not have a legal and binding agreement with acquirer directly. There should be a firm contract between the IPSP and the Sponsored Merchant. Under no circumstances can the financial liability of the IPSP be transferred to the Sponsor Merchant. One may wonder why sponsored merchants are required in the entire landscape or what prevents the sponsored merchants to directly contact the acquirer?

Visa has a Merchant Category Code (MCC) 5967 which is “Direct Marketing – Inbound Teleservices Merchant. This category has to deposit huge reserves with the acquirer, which will be blocked as long as the business is running. Over and above this, maintaining a direct account has its own hassles. As the name of IPSP suggests, the sponsored merchants will mostly be merchants selling digitized and tele-marketing products.

However, based on annual sales of the sponsored merchant, a merchant may be eligible for becoming a direct merchant for e.g. in case of Visa any sponsored merchant whose annual sales exceed USD 100,000/- must enter into a direct merchant agreement directly with the acquirer.

Besides this, the IPSP also has certain business restrictions in terms of geography. The card service provider like Visa can enforce cross-border restrictions on registration of the Sponsor Merchant. For .e.g., as per Visa guidelines, the sponsored merchant should be located in the same Visa region as the IPSP. So, an IPSP such as Epoch is in the US Epoch cannot register a sponsored merchant from France. However, this restriction can be easily overcome by Epoch by creating a new company/subsidiary Epoch EU to cater to the EU– (European Union) Sponsored merchants.

d. Obligations of IPSP

As the liability of sponsored merchant is being transferred to the IPSP, the IPSP also needs to be extremely careful in dealing with sponsored merchants. The IPSP is governed by Visa and has to adhere to Visa guidelines.

Some of the key responsibilities on the part of IPSP are

- An IPSP cannot contract with another IPSP.
- It will terminate a sponsored merchant if required by acquirer or Visa
- It will ensure that the terminated merchant is not permitted to be a sponsored merchant (there are certain pre enrollment checks that need to be made with regard to terminated merchants — this is one of the high fraud prone areas)
- It will include payment acceptance requirements as specified in the Visa International operating regulations in its contracts with its sponsored merchants and ensure compliance by the sponsored merchant

- Ensure that the right merchant category code is issued to the sponsored merchants. Even transactions tagged to the right category have to be ensured by the IPSP.
- It will provide all transaction reporting of the sponsored merchant to the acquirer and Visa on demand.
- An IPSP in the US specifically cannot entertain a merchant in merchant category code (MCC) mentioned below. (This is specific to Visa. Master Card may have its own list of sub-merchants that may be prohibited).

MCC	**Merchant Description**
4814	Telecom Merchants
5912	Non-Face to Face Prescription Drug Merchants
5962	Direct Marketing Travel Related Arrangement Services
5966	Direct Marketing Outbound Telemarketing Merchants
5968	Subscriptions
5969	Direct Marketing-Other Direct Marketers Not elsewhere classified

- All merchants belonging to this MCC have to register as a direct merchant.
- An IPSP cannot operate as a sponsored merchant of another IPSP.
- An IPSP cannot enter into a transaction on its own behalf.

e. Direct Merchant Enrollment

A card issuer has the responsibility to ensure the identity and the risk profile of the constituent. Similarly, in case of a merchant, the acquirer has the responsibility of verifying the credentials.

The acquirer must ensure that the prospective merchant is financially responsible and the merchant will adhere to the Visa International Operating Regulations as well as the applicable local laws.

Other aspects to be looked into by the acquirer include:

- Credit report of the prospective merchant
- Credit check, reference checks and background investigation of the merchant: in addition the credit check of the promoter/proprietor/partners should also be done. Credit check may not always be required if the prospective merchant is a public sector or a private sector company with a specified turnover and has audited balance sheets in place.
- Personal and business financial statements
- Income tax returns
- Physical inspection of the premises and infrastructure to ensure that the prospective customer has the necessary license to carry out the trade and can run the trade.
- Validity check to ensure the member was not terminated previously: this is generally done by software. In case of Master Card, the software is called **M**ember **A**lert **T**o **C**ontrol **H**igh Risk Merchants (MATCH).

The onus of not enrolling a terminated member lies with the acquirer. This has serious repercussions on the acquirer in terms of monetary penalty.

It is the responsibility of the acquirer to hold on record all the documents related to the screening procedure.

f. Merchant Acquirer Agreement

It is mandatory for a merchant to enter into a standard agreement with the acquirer before commencement of operations. The key elements of the agreement will include

- An undertaking by the merchant that he/she will comply with the applicable laws of the land
- He/she will abide by operating regulations of Visa International regarding:
  - Use of Visa owned marks
  - Payment acceptance
- Required acceptance requirement provisions
- The right to terminate the agreement lies with the Visa
- He/she will not knowingly submit any transaction that is illegal or that the merchant should have known as illegal

In case of the US there are additional clauses that have to go into the agreement. The following are clauses that should find a mention in the agreement.

- A merchant must not deposit a Transaction Receipt that it knows or should have known to be either fraudulent or not authorized by the card holder.
- The Merchant is responsible for its employees' actions.
- This covers employee's fidelity and acts and omissions by the employee. The merchant is not absolved by the acquirer in case of frauds.
- Restrictions on Transaction Deposit: The restriction could be in terms of location where the same is to be deposited by the merchant, the period (the number of days) within which the same needs to be deposited etc. The location could be outside the country as well a location within the country. Except for a military

base or International airline, all merchants must deposit the transaction receipts in the transaction country.

There are different time lines defined for deposit of transactions based on the product as well as the nature of the Merchant. Nature of merchant means merchant with multiple outlets or single outlet. In case of multiple outlets, centralization is allowed and in such cases, time lines for deposit of transaction will be higher compared with single-outlet cases.

In case of cruise lines, there are exceptions as they may not be able to deposit within the deadline stipulated. They can deposit at various ports-of-call. Various onboard transactions done by a cruise will be deemed to have been done on the date of deposit of the transaction or the date of disembarkation (if the transaction is deposited at the end of the cruise).

- Prohibitions on transaction processing: One such example could be manual authorizations allowed, per day limits, etc.
- Prohibition on a merchant depositing a transaction receipt that does not result from an act between the card holder and the merchant or the card holder and its sponsored merchant (laundering).

This is a critical control. It is similar to ensuring the end use of funds in banking. One such example could be that the card holder does not buy merchandise from the merchant and instead, cash is paid by the merchant to the card holder directly.

This again can be analyzed through financials of the merchant as well as based on the integrity of the merchant. AML (Anti Money Laundering) rules applicable to banks, are also applicable to the payment card industry.

- Requirements are specified in "Merchant Agreement Requirements - US Region"

- The requirements are specifically laid down in the Visa International Operating Regulation or the respective Card issuer guidelines
- Disclosure of account or Visa Transaction Information prohibitions are specified in "Destruction or Return of Information due to Suspension of Operations - US Region"
- The Card holder Security Program Provisions are adhered to by the merchant and its agents.
- There is responsibility of demonstrating adherence to Card holder Information Security Program
- If a merchant is undergoing a forensic investigation at the time of signing the merchant agreement, it should ensure that the merchant will fully co-operate with the investigation until it is completed.
- **Limited Acceptance.** Limited acceptance means a merchant’s option to accept one category of Visa cards and not another. The two broad categories are:
    - Visa Credit and Business Category
    - Visa Debit Category

The merchant has the option with regard to limited acceptance. The agreement must explicitly specify the limited acceptance option and the merchant’s selection of any of the options.

The agreement also should distinguish all card acceptance related fields, such as pricing and discounting methodology associated with each Limited Acceptance Category.

The fees should clearly distinguish those associated with the solutions company (Visa) and transaction fees associated with other transactions.

- Other provisions can be added by the acquirer in the agreement as long as the provisions are in line with the international operating guidelines of Visa.

- **Specific Merchant Category:** In case of specific merchant categories such as:
  - Health Care Auto Substantiation
  - International Airline merchant
  - Time Share etc.,

There are additional clauses in the agreement that need to be incorporated:

- State the terms required to satisfy payment directly to the merchant, including, but not limited to, the name of the financial institution to which the acquirer, its agent, or sponsored member must deposit funds for payment of Visa transactions.
- The name of the acquirer and his/her location should be clearly stated in the agreement in a letter size consistent with the rest of the agreement in such a manner that it is easily visible to the merchant.
- The acquirer is responsible for maintaining the agreement copy in the file at the acquirer's place of business.
- The agreement has to be signed by both parties.

g. Additional Documentation

Both direct and sponsored merchants have to submit the following documents at the time of signing the agreement.

- "Doing Business As" (DBA) name
- Merchant legal name
- Merchant outlet location, including street address, city, state, and nine-digit ZIP code.
- US Federal Taxpayer Identification Number and identification of the number as either a US Federal Employer Identification Number (FEIN) or Social Security Number (SSN).

- Incorporation status (for example, corporation, partnership, sole proprietor, non-profit, or others).
- Full first and last name, including middle initial, if the merchant is a sole proprietor.
- Merchant Category Code and, if applicable, any secondary Merchant Category Code(s).
- Indication if a merchant is a small and/or disadvantaged business.
- Termination date and reason for termination if the acquirer/merchant relationship is terminated.

h. Merchant Responsibility

All merchants who have entered into an agreement have certain specific responsibility as laid down by VISA. The responsibility may or may not be explicitly mentioned in the agreement. Some of these are:

- Adherence to federal and state laws. This can change from country to country. A Visa merchant in the UK will have to follow different laws compared with a merchant in the US.
- Merchants should accept Visa only for legal transactions.
- They should have the necessary processes and controls to ensure that all associated laws are honored when selling age-restricted products such as alcohol, tobacco etc. Possession of a Visa card does not mean that the card holder is of legal age to purchase the product as issuance of Visa cards is not restricted to individuals over 18 years of age.
- The merchants in the US, who provide services to businesses and government agencies, will have to provide the Tax Identification Number (TIN) to customers. Visa has launched a QPCA (Qualified Payment Card System), which will assist

merchants and customers in reporting seamlessly to the Internal Revenue Service.

- Recovered cards must be returned as per the process defined by the service provider.

i. Merchant Monitoring

The merchant will be continuously monitored both by the acquirer as well as Visa/Master from the risk management and transaction monitoring as well as compliance perspective. The primary responsibility of monitoring lies with the acquirer.

There are a set of Merchant Category codes identified as High Risk by the Visa/Master as mentioned below. These merchants will be closely monitored:

MCC	**Merchant Description**
5962	Direct Marketing-Travel-Related Arrangement Services
5966	Direct Marketing-Outbound Telemarketing Merchants
5967	Direct Marketing-Inbound Telemarketing Merchants
7995	Betting, including Lottery Tickets, Casino Gaming Chips, Off-Track Betting, and Wagers at Race Tracks

j. Merchant Termination

In case of violation of any of the International Operation Guidelines, Visa has the right to instruct the acquirer to terminate the merchant agreement no later than the date mentioned by Visa.

Another key reason for disqualifying the merchant is based on the level of charge back ratio (more on it later).

Visa also has the right to terminate a merchant on the following grounds:

- Undertaking fraudulent activity
- Presenting transaction receipts that do not result from an act between a card holder and a merchant (laundering)
- Entering into a merchant agreement under a new name with the intent to circumvent the provisions of the Visa International Operating Regulations
- Undertaking activities leading to repeated violation of the Visa International Operating Regulations
- Undertaking activities that result in a Regional Office prohibiting the merchant from participating in the Visa or Visa Electron Program.
- Undertaking activities that result in undue economic hardship or damage to the goodwill of the Visa system.

Specific US requirement:

A merchant can be terminated by the acquirer for the following reasons:

- Is convicted for credit or debit card fraud
- Deposited excessive Counterfeit Transaction Receipts
- Deposited excessive Transaction Receipts unauthorized by card holders
- Deposited Transaction receipts of other merchants
- Acquirer received excessive number of charge-back due to merchant’s business practices.

k. Risk associated with merchants

Every business has its own set of risks that need to be controlled. The four Ts of risk management are Treat, Transfer, Tolerate and Terminate.

There are a number of risks associated with merchants. Most of them can be classified as market risk.

The key risks are:

- Fraud risk. This relates to the merchant committing fraud in terms of Bogus Transaction receipts. This could include multiple swiping of the card without proper authorization from the card holder leading to chargebacks. This can be gauged by the chargeback ratio of the merchant.
- Information security compromise by the merchant. There are a number of guidelines issued by Visa /Master etc. with respect to card holder information security. A merchant may collect the card details including CVV2 and pass them on at a cost. It is very difficult to trace and track such issues. Credit card skimming falls under this category.
- Reputation risk is most difficult to handle and it is a consequence of the other risks.
- Compliance risk. Compliance can be classified into external and internal compliance. The merchant may not be able to abide by external compliances.

Internal compliances can be monitored by the acquirer and non-compliance can be addressed by huge monetary penalties.

Certain regulatory compliances such as AML have been dove-tailed in such a manner that the onus lies with the acquirer/payment agent, i.e. Visa. It in turn has built processes and procedures to take care of this.

Both Visa and Master have detailed guidelines on risk management for all participants.

5. Acquirer

Acquirer is one of the key participants in the credit and debit card landscape. In the Amex credit card and Discover Card scenario, the card issuer is the acquirer. This is often a confusing subject and difficult to digest. For e.g. ICICI Bank is a card issuer as well as an acquirer. Similarly Axis Bank too. However an ICICI bank credit card customer can walk into a merchant who is using the POS (Point of Sale) terminal of Axis Bank. The customer will be able to swipe the card and complete the transaction. In such a scenario, the issuer is ICICI and the acquirer is Axis Bank. The merchant may have two POS terminals, one each of Axis Bank and ICICI Bank and the merchant may swipe the ICICI card on the ICICI POS itself. Under such circumstances, the issuer becomes the acquirer.

There are certain interchange fees to be paid if the ICICI Bank card is swiped on Axis Bank POS. The fees will be paid by ICICI Bank to Axis Bank.

In case of Amex Cards, there will be no interchange fees as the issuer and acquirer are the same. This is one of the USPs where a merchant can save in terms of fees. The concept of acquirer and issuer is also commonly used in ATM transactions as well.

Using the same example above, in case of an ICICI Bank card holder using the ATM of ICICI Bank, the acquirer will be Axis Bank (this is also known as third party ATM) and if the ICICI Bank card holder uses the ICICI Bank ATM, the issuer and acquirer are the same.

Interchange fees in case of third-party ATMs were a bone of contention couple of years ago in India. In case of third-party ATM transactions (including balance enquiry), interchange fees were charged to the card holders account. Owing to this disadvantage, a card holder had to find the ATM of the issuer. This scenario changed significantly a couple of years ago in India, when the RBI intervened to make third-party ATM transactions free. After six months, the policy was reviewed and RBI restricted third-party free ATM transactions to five a month. In case of ATM interchange, fees in India are Rs 16 per transaction, which ICICI Bank would have to pay to Axis Bank. The reader must not confuse this interchange fee of Rs 16 with what is charged to the customer (which was Rs 50 earlier, but now it is free up to five transactions a month).

a. Acquirer Types

An acquirer has two dimensions: POS (Point of Sale) and ATM (Automated Teller Machine) acquirer and bank and non-bank acquirers. The bank acquirers are predominant and in majority compared with non-bank acquirers. Non-bank acquirers are common in the US.

The top non-bank acquirers are:

- First Data (POS)
- Global Payments (POS)
- Heartland Payment System (POS)
- Euronet (ATM)

First Data has a long history dating back to 1964. It has been a story of umpteen numbers of mergers, acquisitions and dissolutions. This company vaulted $9.3 billion in revenue with US Payment Transaction Dollar Volumes of $1.25 trillion. It had worldwide merchant locations of 6 million and employees more than 25,000 (Source: www.firstdata.com –First Data Facts)

In India the concept of non-bank acquirers does not exist. Only recently, ICICI Bank and First Data formed a merchant acquiring alliance under the name of ICICI Merchant Services.

b. Acquirer Functions

The services of an acquirer broadly comprise four functions:

- Signing up merchants to accept network branded cards
- Providing means to authorize valid card transactions at client merchant locations, done basically through the supply of POS machines
- Facilitating the clearing and settlement transactions through the payment network
- Supplementary support services like transaction statement generation and dispatch to merchants.

Merchant Acquisition

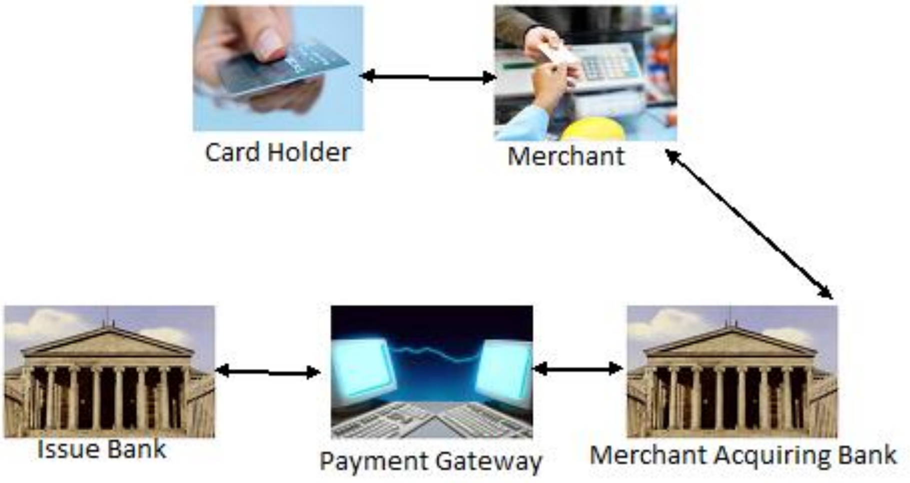
This is one of the core functions of the Acquirer. The more number of merchants, higher is the revenue. However one cannot just sign up merchants at random just to increase numbers. Payment solution providers like Visa /Master etc. issue a set of guidelines issued and the law of the land should also be considered.

The merchant acquisition process of entering into a contract has already been discussed in Section 3 in depth.

Another supplementary service related to the merchant acquisition is the facilitation of the merchant equipment, popularly known as Point of Sale (POS) Terminal. There are multiple business models of POS. In one model, the POS machine is owned by the merchant and in the second business model the acquirer can lease out the POS to the merchant and earn lease rentals. This would be a cheaper option for merchants.

Authorize and Capture Transactions

This the second of the four functions of the acquirer. The transaction flow is as depicted in the chart below.



Authorization is a process wherein the merchant is guaranteed payment for authorized purchases (barring future disputes).When a card is swiped at the merchant's terminal, a request for authorization, along with the cardholder's information and transaction amount is transmitted to the merchant acquirer. The merchant acquirer then forwards the request through the network, which in turn, queries the card holder's issuing bank. The card holder's bank may either approve or reject the transaction based on credit or fund's availability.

Certain precautions and controls need to be addressed while the merchant transmits a card holder's data to the acquirer and then to the issuer. The Payment Card Industry Data Security Standard (PCI-DSS) addresses the security issues. This framework also covers network-related security. (A separate section has been dedicated to PCI DSS).

In case the transaction is approved by the issuer, the issuer confirms the transaction with the authorization code and the amount of authorization is set aside or carved from the available credit or available funds in the card holder’s account. The authorization code is sent from the issuer to the acquirer and then to the merchant’s terminal through the network. Once the authorization code is generated, the transaction is confirmed with the card holder by way of a paper receipt in duplicate with a signature.

The paper receipt environment in India is different from the US. In the US, as per regulation, paper receipts are not required for transactions less than USD 25 and for Debit Card transactions less than USD 15 (Federal Reserve Regulation E).

It is interesting to note that authorization does not lead to actual collection of funds at this time. Authorization is only a confirmation that the issuing bank agrees to a future settlement.

Clearing and settlement

This is another core function. The process of collecting funds from the issuing bank to the reimbursing merchant is known as clearing and settlement. (This is dealt with in more detail in the transaction section).

Supplementary support Services

There are number of supplementary support services in and around the three functions such as transaction statement generation of the merchants and answering to merchant queries etc. In addition to this, the acquirer also monitors and reports the various types of reports and analyses the same. Some of the key transaction-related monitoring requirements are discussed in the sections below.

c. Acquirer Responsibility

The acquirer has a number of responsibilities that are guided by local laws as well as guidelines and rules of payment services providers. The responsibility is basically classified into two categories viz.

- Merchant Acquisition Related
- Merchant Transaction Related

1. Merchant Acquisition Related Responsibility

Jurisdiction Restriction

Each Payment service provider such as Visa/Master has defined the jurisdiction within which the acquirer can acquire merchants. For e.g. a US acquirer cannot acquire a merchant in India and vice versa.

There are certain exceptions to this rule and Visa/Master defines these exceptions. In case of Visa, cross-border transaction between US and Canada is allowed subject to certain conditions.

Due Diligence

An acquirer must undertake due diligence before entering into a contract with the merchant. One of the due diligence activities is the Terminated Merchant File Query before enrolling a merchant. The acquirer carries out this due diligence before signing up the IPSP. The IPSP also undertakes this exercise before entering into an agreement with the sub-merchant.

Following acquisition of the merchant, a number of responsibilities vest with the acquirer. The card provider defines these responsibilities.

Control Policy

Each acquirer must implement, underwrite, and monitor the control policy, which should be approved by the board

Merchant Notices

If the acquirer is served any notice by any regulatory authority, with respect to a merchant or the acquirer comes to know of a potential bankruptcy or regulatory proceeding involving one of its merchants, it must ensure the following:

- Monitor those proceedings to ensure that no legal relief is being sought that would interfere with the chargeback process
- If such a relief is being sought, to the best of its ability, oppose that relief
- Notify Visa as soon as possible but no later than close of business on the next business day following such a discovery

  An Acquirer that fails to comply with the requirements of "Acquirer Responsibility for Visa Transactions — US Region" is subject to penalty and termination of membership or both.

Merchant Diversification

An acquirer cannot put all the eggs in one basket i.e. an acquirer cannot have all his clients in one single Merchant Category Code (MCC). This is a high-risk scenario. Visa/Master defines the minimum level of diversification. This is one of the risk management measures.

Training and Education

The acquirer must train and educate merchants on the corporate policy and ensure that they comply with these**.**

2. Merchant Transaction Related Responsibility

Merchant transaction related responsibilities are more in number compared with acquisition related responsibilities.

Transactions can be broadly classified as domestic and cross border for the purpose of monitoring. (There are various ways of classifying a transaction. More of this is covered in the transaction Section). Some prominent transactions are discussed here.

Prohibition of Illegal Transactions

It is the responsibility of the acquirer to ensure that its merchant outlet, agent, or IPSP does not process illegal transactions. The acquirer is subject to corrective action and fine as defined by the payment service provider.

In case of illegal cross border transaction activity, the fines are more stringent. The below mentioned table provides a fair idea of the quantum of penalty which Visa levies on the acquirer.

Table A –Penalty by Visa on illegal Cross border activity:

Violation	Month	Visa Action or Fine
Warning	First month in a 12-month period	Warning letter requesting response with specific date for correction
Uncorrected Violation	Second month in a 12-month period	US $25,000 fine per Merchant, Merchant URL, Sponsored Merchant, or Sponsored Merchant URL identified

Uncorrected Violation	Third month in a 12-month period	US $50,000 fine per Merchant, Merchant URL, Sponsored Merchant, or Sponsored Merchant URL identified.
Uncorrected Violation	Fourth month in a 12-month period	Visa may permanently disqualify the Merchant, Sponsored Merchant, or IPSP from participation in the Visa Program.
Uncorrected Violation	Fifth month in a 12-month period	Visa may prohibit the Acquirer from contracting with a new Merchant for a period of one year or impose some other sanction.
Source: Visa International Operating Regulations		

- **Merchant Weekly Activity Monitoring**

The acquirer has to monitor the following on a weekly basis

- Gross Sales Volumes
- Number of Transaction Receipt Deposits
- Gross amount of weekly deposits
- Average Transaction Amount
- Chargeback

- **Merchant Exception Reports**

The acquirer must have processes in place to generate the following exception reports:

  - Current weekly merchant gross sales volumes equaling or exceeding US $ 5,000, or local currency equivalent, and any of the following exceeding 150% of the normal weekly activity
  - Number of weekly Transaction Receipt Deposits
  - Gross amount of weekly Deposits
  - Average Transaction Amount
  - Number of weekly chargebacks.

- **Merchant Chargeback Activity Monitoring**

The acquirer must monitor the chargeback to transaction volume ratio of its merchant and identify any merchant that receives:

  - More than 100 chargeback transactions per month
  - Exceeds the charge back-to-transaction volume ratio of 3%

- **Chargeback Rate Acquirer Standards**

This is one of the performance standards, which the Payment Solution Provider such as Visa monitors closely.

For e.g. in the US, the following rules apply for VISA.

  - An acquirer must not exceed the chargeback rate for the respective card programs specified for each category of merchants.
  - In case of Department store it must not exceed 0.17 %.

- A chargeback rate is the number of chargebacks received as a percentage of all transaction receipts processed. (Chargebacks are discussed in the transaction section)

Data Quality Compliance Standard

It is the duty of the acquirer to ensure that all authorization requests and clearing records contain complete data. If data is incorrect or missing, the acquirer may be subject to the Data Quality Compliance program of the payment service provider.

Visa imposes stringent penalties and fines in case the acquirer does not adhere to the data compliance standards. The penalties could range from a one-time penalty of USD 5000 up to USD 25000 per month.

d. Appointment of Agents

In common parlance, an issuer of the card or the acquirer is together commonly referred to as the participant. Participants may not be in a position to handle all the process-related activities by themselves and may use services of a third party. This third party is also called agent (both these words are used interchangeably), since the contractual relationship between the participant and third party is of Principal-Agent.

In the US region, for Visa, the definition of Agent is “An entity that acts as a Visa Net Processor, third party or both”. A Visa Net Processor (VNP) is an entity that is directly connected to Visa via a Visa Net Extended Access Server. A third party VNP is neither a Visa acquirer nor an issuer. Neither the Visa issuer nor the Acquirer owns the processer.

Service Provided by Agents to Members

In addition to the VNP, the service provider may provide a number of other services. Master card places services providers into two broad categories:

- Independent Sales Organization (ISO)
- Third Party Processor(TPP)

An ISO provides ISO Program service. A program Service includes but is not limited to:

- Merchant Solicitation
- Card Holder Solicitation
- Customer service

A Third Party Processor (TPP) provides TPP service. Master Card further classifies a TPP as Category-I TPP or Category-II TPP.

A TPP Service program includes and is not restricted to:

- Terminal Operation
- Authorization Routing
- Voice Authorization
- Call Referral Processing
- Electronic data capture
- Clearing file preparation and submission
- Settlement Processing
- Card Vendors

e. Third-Party Management Responsibility

The responsibility of third-party management vests with the participants and the third party.

Participant Responsibility

The participants (issuers and acquirers) are responsible for all errors, acts and omissions of such third parties, including their agents and vendors.

Third-party service providers also have to enter into necessary contractual agreements with acquirers. The documentation will be as defined by payment service providers such as Visa/Master.

Points to be noted by members in such agreements are as follows:

1. Conduct background investigation before contracting a third party;
2. Before entering into a contractual agreement, a participant must contact Visa to query the Agent Reference File.US specific requirements: It is interesting to note that the information flow on third party is one way from the participant to Visa. It will not provide details of an existing third party relationship with other members or their identities to an enquiring member. If another participant has discontinued its relationship with a third party, Visa refers the enquiring member to one with a former relationship for further information. However, the former member is not obligated to disclose information to the enquiring member. Registration of a third party in the US Agent Reference File does not represent confirmation of the agent's compliance with a specific visa requirement.
3. Execute a written contract with an agent and ensure that the agent meets the minimum standards as specified by Visa/Master. US specific requirements: The agreement must be signed by the senior officer of the participant. The agreement

must have a termination clause if the third party participates in an activity prohibited by Visa or the participant or its merchant becomes insolvent.

4. Have written policies and procedures for evaluating and approving third parties and VNP. These policies and procedures must meet the minimum standards as defined by Visa/Master.
5. Distribute these policies and procedures to the VNP and third party.
6. Verify that the senior management has the necessary expertise in terms of knowledge and experience to successfully perform the contracted services.
7. Conduct physical inspection of the business premises to:
   - Verify inventory
   - Review solicitation or sales material
   - Inspect operational controls
   - Monitor security standards regarding unauthorized disclosure of, or access to, Visa sensitive data and other payment system transaction information.
8. Ensure all VNP and third parties comply with the applicable Visa requirements, including but not limited to:
   a. Adherence to PCI DSS standard
   b. ATM deployment and operational support as defined by Visa
   c. PIN entry device deployment and operational support compliance with Pin management requirements.
9. Maintain necessary files containing full applicable documentation. This file has to be preserved for two years following discontinuance of the agent.

   US specific requirements: The participant must inform Visa, through an online channel, any change in a third party's principal or business relationship including change of ownership or termination of contract. This must be done within three business days of the change or knowledge of the change.

Participants may be required to provide documentation to confirm compliance with the guidelines of Visa.

Participants must conduct an annual review of all third parties to conform to ongoing compliance with the risk standards. Participants must submit a detailed quarterly report regarding the activity and services of each third party doing business on its behalf in the format specified by Visa; it should be signed by an authorized officer. In the event of non-submission of the same within 30 calendar days from the quarter end, Visa will impose necessary fines.

Agent Responsibility

The agent must not:

1. Present to the prospective customer (card holders and merchants) under any other trade names except the one registered with the member.
2. Appear to be a member of Visa unless the agent is an existing member.

6. Issuer

As already discussed in the first section, an issuer is one who issues the respective cards to the constituents.

Issuers can be classified based on the nature of the issue of the card.

The issuer is also called the issuing member and the terms are used interchangeably.

In case of Master Card, there are three types of members;

- Associate Member
- Principal Member
- Affiliate Member

As per the rules of the Master Card, the Principal member can only be a financial institution.

a. Types of Issuers

Issuers are financial Institutions who issue the cards. These financial institutions could be banks or non-banks. An example of a non-bank is GE Money, which also issues cards. One set of cards are called white label cards. The issuer is a non-bank entity. For example, Reliance Money Card could be a white label card. The actual issuer of the card would be Citibank. But Citibank’s name does not feature anywhere on the card.

b. Member Responsibility

Adherence to Rules and regulations

A US member must comply with:

- US regional operating regulations
- Applicable certificate of insurance and By-laws

- Visa international operating regulations
- Visa product brand standards
- Payment technology standards manual
- Visa net manual

Emergency variances to a specific regulation can be granted by Visa if the member is not able to comply due to circumstances beyond control such as natural disasters, war, government restrictions due to political unrest, or failure of Public infrastructure. These variances cannot exceed for more than 120 days without consent of Visa.

Confidentiality requirements

- The member must not disclose any confidential information.
- Store and handle confidential Information in a way that prevents unauthorized disclosure.
- Disclose confidential and proprietary information only to those employees on a specific need-to-know basis.

An issuer has a number of responsibilities in the life cycle of a card. Some of the responsibilities have already been discussed in earlier sections. For aggregation purposes, it is summarized below.

c. BIN Management

One of the key responsibilities of a member includes BIN Management and handling BIN in a careful manner. The first six digits on the card including Major Industry Identifier (MII) is commonly referred to as **B**ank **I**dentification **N**umber (BIN). It is also called **I**ssuer **I**dentification **N**umber (IIN).

.

As already discussed, major card issuers' BINs are as follows:

Issuer	**Identifier**	**Card Number Length**
Diner's Club/Carte Blanche	300xxx-305xxx, 36xxxx, 38xxxx	14
American Express	34xxxx, 37xxxx	15
VISA	4xxxxx	13, 16
MasterCard	51xxxx-55xxxx	16
Discover	6011xx	16

A BIN is licensed by Visa. A BIN licensee is defined as an entity which is a member of, and is allocated responsibility by, Visa for a specific BIN as specified by the VISA USA Inc. Certificate of Incorporation and By-laws and US Regional Operating Regulations. An issuer and an acquirer are equally responsible for the BIN licensed to them.

Every issuer is issued a BIN range and can use only those numbers. The issuer cannot issue any BIN to any card. This is governed by Visa.

1. BIN License

Visa classifies its members into three classes:

- A principal type member
- A associate type member
- A participant type member

A principal type member must only use a BIN for which it has the license.

An associate type member may license its own BIN, or use a BIN licensed to its sponsor.

A participant type member must use a BIN licensed to its sponsoring principal.

A principal or associate must submit a “BIN License agreement” to Visa before issuing any card bearing the requested BIN or acquiring a merchant using the BIN. By completing the BIN License agreement, the member acknowledges that it will use the requested BIN only for the purpose specified in the request. A member must submit a revised form to reflect any change in use before the effective date of change. There is a standard license agreement.

Visa licenses BINs must be used for issuing, acquiring, processing and other approved activities; the BIN licensee must use BINs only for the purpose for which the BIN Licensee is approved.

US Specific:

A Visa BIN may be used for non-visa purposes such as private label card programs, but members must seek specific approvals from Visa. The request for the same has to be made in writing by the member, stating the program objectives and filling up the BIN License Agreement.

2. BIN sale or exchange:

A BIN licensee must not sell, rent or exchange any BIN. However, Visa may, at its sole discretion, accommodate requests for BIN transfers in connection with a portfolio sale. A portfolio sale can occur due to a merger or acquisition. For example, ABN Amro Bank sold to Royal Bank of Scotland. If ABN and RBS have separate BINs, the ABN BINs will be transferred to RBS by express permission of Visa.

Another example of portfolio sale could be a bank selling its credit card portfolio to another bank, similar to selling of a retail loan portfolio. In such cases, which results in a change of BIN, licensee or user must notify Visa within 10 calendar days of the portfolio sale or transfer by submitting a “Change of BIN Licensee /User” request to Visa.

Visa holds the selling institution financially liable for all portfolio activities, in addition to payment of all applicable fees, until Visa acknowledges all required documentation.

3. BIN release

If a member thinks that it may not require a specific BIN, the same can be released to Visa. This is done by submitting “Release of BIN” request. A member must not use a BIN recalled by Visa after the recall effective date. However, before the effective date the member may want to cancel the BIN release. This is also possible via filling up of the requisite form by the member.

4. Membership Downgrade-BIN requirement

A principal type member or associate type member may be downgraded to participant type member status. In case of such downgrades, the principal type or associate type must either:

Return its licensed BIN to Visa by submitting a “Release of BIN” request before the effective date of change; or

Transfer its licensed BINs to its sponsor by submitting the “Change of BIN/Licensee /User Request”.

5. BIN Recall/reassignment:

Visa has the right to recall a BIN. In the event of recall of a BIN in the US by Visa:

The BIN is eligible for deletion from VisaNet six months after the following events, whichever happens last:

Expiration date on the last card

Cease of date acquiring activities

Cease of date processing activities

The BIN may be subsequently assigned to another merchant following deletion.

The original BIN licensee will continue to remain liable for any exception related to transactions generated on the BIN before deletion.

The BIN licensee is responsible and liable for any recalled BIN until it is fully deleted from all VisaNet Systems.

6. Voluntary Membership Termination:

If a member decides to terminate the membership voluntarily, the member will be terminated by Visa only after:

- All BINs are deleted from VisaNet systems
- All BINs are transferred to another BIN Licensee

7. Unique Identification with Account Number:

An issuer using a BIN licensed to its sponsoring member must be uniquely identified with the first 9 digits of the account number.

.

d. Card Manufacture and delivery

This is also a key function of the issuer. Generally, the Issuer does not have the capability in-house to cater to this requirement as it is not the core competence of the issuer. An issuer may contract through any other issuer or a distribution channel vendor for packaging, storing, and shipping of pre-manufactured products. A pre-manufactured product is a non-personalized card that is already manufactured, encoded, and embossed/printed and is ready for sale or distribution to card holders.

A distribution channel vendor is also a third party and needs to undergo the process related to a third party. The processes include:

- Registering the vendor as per the third party agreement
- Validate annually the third party's compliance with Global Physical Security Validation requirements for data preparation, encryption support and fulfillment card vendors
- Comply with the third party agent program requirements.

1. Card Security Staff Requirements

An issuer must have qualified fraud control and card security officer and staff that are primarily responsible for all areas of security for cards. The job description of a security officer includes the following:

- Investigate all fraudulent use of cards
- Plan and supervise manufacturing, embossing, encoding, printing, and mailing of the issuer's cards
- Plan and supervise physical protection of the issuer's center and building
- Participate in center employee background investigations.

Specific US requirements:

An issuer must enforce accountability controls throughout the manufacture and card personalization process and resolve all discrepancies. It must ensure that the manufacturing, embossing, encoding, hot stamping, electronic imaging, and mailing of cards are completed in an area restricted to people responsible for, or engaged in, the production and operations and they must comply with the following:

- Security Validation requirement for card vendors
- Logical security validation requirements for card personalization vendors
- Creation and maintenance of a secure environment.

2. Adhesive Material on Cards:

An issuer must ensure that no adhesive material is affixed to either side of the card unless it is integral to the manufacture of the card.

3. Card Activation Sticker:

A US issuer may affix a card activation sticker to the front or back of the cards, if the sticker does not interfere with any other security features of the card.

4. Pin Issuance Requirements

An issuer must make a PIN available to each card holder for use with a card, except that PIN issuance is not required for specific type of prepaid cards.

An issuer must:

- Notify its card holders of PIN availability
- Comply with the Payment Technology Standards
- Successfully complete required testing to demonstrate the capability to perform PIN verification, or designate Visa to perform this function
- Ensure the security of the PIN.

5. Expiration Date Standards

It is the responsibility of the issuer to ensure the expiration date standards specified by Visa/Master etc. are adhered to. There should be absolute integrity on the expiry date printed on the magnetic card and the chip.

In case of chip cards, the expiry date on the card should not exceed the issuer's public key, or any security feature containing an expiration date in a chip if one is present on the card.

In case of non-personalized cards, which do not carry a cardholder name, the expiry date should be restricted to a specific period from the date of issuance.

e. General Issuer Requirements

1. Blocking funds with third party

A US issuer must not issue or reissue a Visa card that accesses funds on deposit at an organization other than the issuer's unless it:

- Receives prior written consent from the organization where the funds are deposited
- Completes Automated Clearing House (ACH) notification requirements.

An example: The Operative account is with Citibank and a Debit card is issued by Well's Fargo based on the balances in the Citi Bank account. This is slightly risky in terms of credit risk. Hence, Visa insists on a written consent. Even if a written request is obtained there may be certain processes and documentation requirements between both.

ACH is a type of clearing system prevalent in the US. In an ACH notification, the card holder notifies the bank on debiting the account based on the card issuer's instructions.

2. Exchange Rates:

An issuer must provide complete written disclosures of any fees that may be charged to a cardholder for an international transaction or when currency conversion occurs. A US issuer must disclose to each of its cardholders in writing that the exchange rate between the transaction currency and the billing currency used for processing international transactions is either:

- A rate selected by Visa from the range of rates available in wholesale currency markets for the applicable central processing date, which may vary from the rate Visa itself receives, or
- The government-mandated rate in effect for the applicable Central Processing Date; in each instance, plus or minus any adjustment is determined by the issuer.

3. Charges and Fees:

It is the responsibility of the issuer to ensure that the charges and fees are communicated to the card holder through a written communication.

US Specific requirement:

If an issuer charges an application fee, it must disclose the same and explicitly mention that this fee is over and above charges payable on the Visa Card. The issuer must also provide a disclosure that allows the cardholder to avoid the fee in case of no intention to pursue the application. The issuer or its agent must not charge a fee for providing the application to a potential Cardholder.

4. Unsolicited cards prohibited:

In the US, issuance of unsolicited cards is prohibited. They should be issued to a prospective cardholder who has requested the card on application and met all application and card issuance requirements.

5. Limitation Period on notification of unauthorized card transactions

An issuer has to notify the card holder that the notification of unauthorized transactions has to be received within 60 calendar days of the mailing date of the first statement showing unauthorized visa transaction.

6. Other notification (Specific to the US):

- The card holder should be explicitly notified that the card must not be used for any unlawful purposes.
- The issuer must advise the card holder to immediately sign on the signature panel on the back of the card.
- The issuer must disclose in its cardholder agreement that it may provide cardholder personal data to Visa, its members, or their respective contractors for the purpose of providing emergency cash and emergency card replacement services. It also requires the cardholders' consent to release this information.

An issuer must provide a toll-free telephone number where a card holder may obtain assistance on round-the-clock, especially when he/she is travelling. The same needs to be printed on the back of the card, or on any other promotional material.

- All upgraded features need to be disclosed to card holders in a timely manner.

7. Chip Card related requirements

As mentioned in section one, magnetic stripe technology is gradually being replaced with chip cards. In Canada, chip cards have become mandatory from September 2010. From the issuer perspective, a number of rules need to be adhered to in a chip-based card. Visa has come out with certain guidelines on the same.

An issuer of cards bearing a chip must:

- Comply with the Visa Integrated Circuit Card specifications (VIS).
- Ensure any chip used to facilitate Visa payment services complies with the Visa Chip Security and service level Standards.

- Ensure that its chip card meets the EMV Integrated Circuit Card specifications for payment systems.
- Ensure the chip must be in the front of the card.
- Comply with the ISO standards 7816-2 Reference Number ISO/IEC 7816-2:1988 (E) - "Identification on Cards-Integrated Circuit(s) Cards with Contacts-Part 2: Dimensions and Locations of the Contacts".
- Perform and be capable of acting on the results of validation of EMV – online card authentication cryptograms for all chip initiated authorization messages processed through VisaNet.
- Notify Visa of its intention to use chip technology at least 60 calendar days before issuance.
- Ensure magnetic stripe 2 information and the card holder name from Track 1 is contained in the chip. Other Track 1 discretionary data is optional.

A chip card may facilitate access to non-Visa services provided that:

- The services do not compromise the security or the functional integrity of the Visa Smart Payment applications.
- Additions of the services are managed and controlled by the issuer or its sponsored member.
- Issuer indemnifies Visa from all claims or losses resulting from Non Visa Services facilitated by the chip card.

Another interesting outcome of the chip card technology is the convergence of the card. One can use the same smart chip card for a service within an issuer i.e., one can have a Visa Platinum Card and a Visa co-branded card with an airline from the same issuer, say Citibank. Another example could be a Diners Club Card and Visa Platinum Card, both from Citibank. In case of multiple account numbers in a chip card, the issuer:

- Must allow the card holder to select the service and account to be used for a transaction as permitted by local law, and as specified in the US Regional Operating Regulations.
- Designate an account number for each account accessed by a Visa Smart Payment Application. In addition:
  - The chip may contain multiple application number
  - The Visa Payment application may provide access to more than one account.
- Specify an alpha numeric name for each funding account facilitated by the Visa Smart Payment Application, when the chip provides access to more than one account, as specified in the VIS.

One of the critical success factors of the chip-based cards is interoperability. The issue of interoperability was addressed by a standard called EMV. It is a technical specification developed jointly by **E**uroPay International, **M**asterCard International and **V**isa International, to provide standards for processing debit and credit transactions and ensure global interoperability for the use of chip technology in the payment industry.

In case the chip is not able to adhere to the interoperability issues, the card becomes unusable. It is the responsibility of the issuer to ensure that chip cards are interoperable. Visa has come out with a program titled “Chip Interoperability Compliance Program”. Visa can enforce this program on the issuer if it identifies that the issuer has highly severe chip interoperability problems. There are heavy monetary penalties for non-adherence to this compliance program.

7. Regulation and Compliance

1. Introduction

The philosophy of regulation is to protect consumer interest and ensure that firms participating in the business do not exploit customers and make undue profits. Regulation is also necessary to ensure that business is conducted in a fair and transparent manner. Hence, every industry and market must be regulated to a certain extent.

In recent times, one of the drivers for regulations has been failure or collapse of financial systems and its widespread impact on the economy. One example is the Sarbanes Oxley ACT of 2000, which was an outcome of the Enron Scam.

Regulations can be classified as 'Self-Regulation' and 'Regulation by Statute'. Self-Regulation, as the word indicates, is a regulation by itself. They are referred to as SROs, which are not prevalent in the cards industry.

Regulations are normally passed by an act of the Parliament or an Ordinance from a regulatory body such as FRB. These are lengthy procedures with legal requirements and may vary across countries. Generally, a regulation in a preliminary stage is referred to as a bill. Once the bill is passed by the Congress in the US, it becomes an act. Sometimes it may take years for a bill to be passed as there are other pressing priorities for the government. In case the Congress is not in a session and an emergency regulation needs to be passed, the government can promulgate an ordinance. Once the ordinance is passed, it becomes an act.

Regulations are dynamic in nature and they can change based on the business environment. Regulations need to be amended intermittently so that they are relevant to the current environment. A fine balance should be maintained between over-regulations and under-regulations. Over-regulations can hamper business activities and under-regulations would be ineffective.

Other aspects of regulations are costs of implementing them and time taken to set controls and checks in place. Considering implementation of the Sarbanes Oxley Act in the US, it was a huge monetary burden on small companies and there is a debate on whether to have a lighter version of the act for small and medium enterprises.

Regulations in the US have a very peculiar structure; they are dual in nature. The first level is Federal Regulations, which encompass the US. Then, there are State Regulations that are applicable to specific states in which entities or businesses operate. These are sometimes referred to as Federal Laws and State Laws.

India also has such a structure in certain items, which are referred to as the concurrent list in the Indian Constitution.

2. Regulation vs. Supervision

Regulation and supervision are two sides of the same coin. The regulator, at the time of forming a regulation, must include controls, checks and balances required in the industry.

It is not enough to lay down what is to be done; it is also important to ensure that it is being done. This is the role of supervision. It is not necessary that the regulator undertake the supervisory role. All over the world, there is a hybrid mode of supervision. Some elements of supervisory powers are retained at the regulator level, while some are empowered with certain other bodies that may or may not be under direct control of the supervisor.

It is only through supervision that a regulator comes to know whether regulations are complied with or no. It is not possible to identify non-compliance unless regulations make it mandatory to disclose events/incidents to the regulator/consumers/investors. Hence, supervision is the key to ensure compliance to regulations.

Non-compliance is viewed seriously by a regulator. Non-compliance can be minor or major based on the impact on majority of stakeholders. Globally, huge penalties are levied for non-compliance. Penalties are especially high in the US. A penalty could range from a few thousand dollars to temporary or permanent suspension of the non-complying body.

3. Generic vs. Specific Regulations

A regulation may be specific to an industry such as the Credit Card Accountability Responsibility and Disclosure (CARD) Act of 2009, which is specific to the lending industry and is aimed at modifying the parent Act, “Truth In Lending”. The latest specific act, aimed at the capital market, but with some reference to the credit card industry as well, is the Dodd Frank Wall Street Reform and Consumer Protection Act, which came into effect in the US in July 2010. A generic regulation can span across industries. An example of a generic act is the USA Patriot Act 2001.

It is easy to identify those acts that are directly related to the industry, but it becomes difficult to identify generic laws. Legal experts are required to read the fine print and understand generic laws and interpret whether they are applicable to the specific industry or no.

4. UK Regulators

The UK has a different regulatory structure compared with the US and India. There is a single regulator in the UK called the **F**inancial **S**ervices **A**uthority (FSA). However, in India and the US, there are different regulators for different purposes.

Recently, it was reported in the press that the FSA is being abolished. One may wonder how it would be possible to dismantle the regulatory aspect of this business considering the expansion of the financial services industry. Abolishing of the FSA is only one side of the story. There are other implications of this.

Future of FSA: Chancellor George Osborne, in June 2010, announced a series of wide-ranging reforms to transform the UK's financial regulatory landscape by 2012. One of the recommendations was to abolish the FSA and bolster supervisory power of the Bank of England. The macroeconomic issues will be handled by an independent Financial Policy committee at the bank. The government also plans to set up a new consumer protection and market authority to oversee authorized financial firms offering services, including financial intermediaries, and their business conduct. A separate agency, "Serious Economic Crime Agency", will be set up to tackle financial crime. The complete speech of Mr. Osborne is available at http://www.hm-treasury.gov.uk/press_12_10.htm.

It will be interesting to see how the UK regulatory landscape shapes up in the next couple of years. It might end up with different regulators for different purposes.

FSA in the current form: The FSA is an independent non-governmental body, which has been given statutory powers by the Financial Services and Markets Act 2000 (FSMA). The Company is limited by guarantee and funded by the financial services industry. The Board is appointed by the Treasury. The objective of the FSA was envisaged as follows:

- Market confidence
- Financial stability
- Public awareness
- Consumer protection
- Reduction of financial crime

FSA has been given wide-ranging powers of rulemaking, investigatory and enforcement to meet the aforementioned five statutory objectives. The FSA regulates the financial services markets, exchanges and firms. It sets the operating standards and it can take punitive action against those that fail to adhere to these standards.

FSA (as of November 2010) regulates more than 29,000 firms. It was given additional powers in the recent past. Since November 2004, it has also been entrusted with regulating the mortgage business. Since January 2005, the general insurance industry is also being regulated by the FSA. Moreover, it has been regulating the conduct of business of banks and building societies, including payment services, since November 2009.

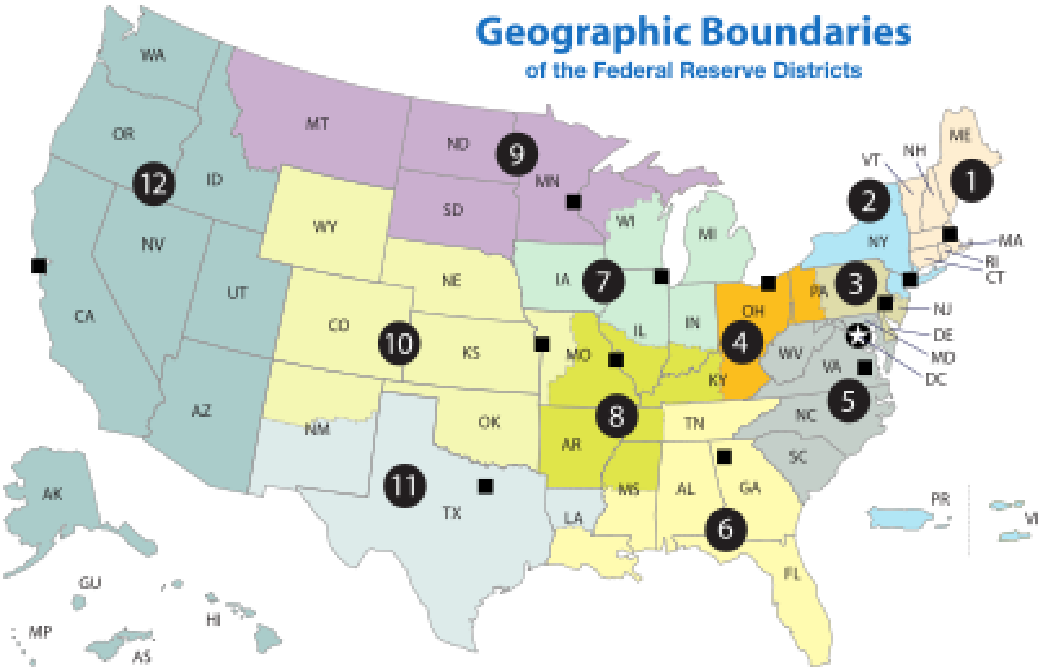
5. US Regulators

The US has a number of regulators:

Srl	Regulator	Objective
1.	Federal Reserve (The Fed)	The structure of the Federal Reserve, the central bank of the US, is quite unique. It has a dual structure: Federal Reserve and regional Federal Reserve. There are 12 regional Federal Reserve banks as indicated below.
2.	Federal Trade Commission (FTC)	Established in 1914, under the Federal Trade Commission Act; it is an independent agency with a mission to protect consumers and eliminate unhealthy practices.
3.	Financial Crime Enforcement Network (FINCEN)	It was set up under the US Treasury. It collects and analyzes financial transactions to combat money laundering, terrorist and other financial crimes.

One of the drawbacks of multiple regulators is that there can be overlap of jurisdiction that can lead to ambiguity.

The map depicts locations of regional Federal Reserve entities in the US:



6. US Regulations

There are innumerable Regulations that the cards and payments industry's market participants need to adhere to. Some of them are direct and some are indirect. The key regulation that needs to be adhered to is summarized below:

i. Truth in Lending 1968 - Regulation Z

This is one of the oldest regulations in the US. It is also called TILA; it was enacted in 1968 and it became effective on July 1, 1969. It was amended in 1970 to prohibit unsolicited credit cards. It was further amended by the Fair Credit Billing Act of 1974. Truth in Lending Act is implemented by Regulation Z. TILA is applicable to both open-ended credit and close-ended credit. An example of open-ended credit is credit cards. The purpose of TILA is to ensure that credit terms are disclosed in a manner in which a consumer can compare the credit terms readily and knowledgably. All creditors must use the same credit terminology.

The Act:

- Protects consumers against inaccurate and unfair credit billing and credit card practices
- Provides consumers with recession rights.

The Finance charge computations also need to be provided by the issuer.

ii. Equal Credit Opportunity-Regulation B

Regulation B prohibits creditors from discriminating on the basis of age, sex, race, color, religion, national origin, and marital status.

In the event of the credit card being rejected by the issuer, the notification of rejection has to be given in writing and the reason for rejection must be mentioned specifically. If an applicant was denied due to adverse information on the credit bureau report, the applicant is entitled to receive, at no cost, a copy of the bureau report.

iii. Fair Credit Reporting Act (FCRA) 1970

The objective of this act is to promote the accuracy, fairness and privacy of information in the files of consumer reporting agencies. These include credit bureaus and other third-party agencies.

One confusing feature of the US regulation is that an amendment to an existing regulation is also referred by a new name. A new regulation, **Fair and Credit Transaction Act of 2003 (FACT),** was passed to amend the Fair Credit Reporting Act. The key objectives of FACT were:

- Prevent identity theft
- Improve resolution of consumer disputes
- Improve accuracy of consumer records.

If one happens to read the FCRA, one would find that it contains the amendments made through FACT as well.

Highlights of FCRA:

- Right to be informed that the credit report has been used against a prospective credit card applicant (other conditions also exist); the applicant should be provided with full details of the agency that provided such information.
- Right to know what is in the credit file, free of cost under certain circumstances, and at least once in 12 months for free.
- Right to ask for a credit score.
- Incomplete or unverifiable information must be deleted.
- Outdated negative information may not be reported. Negative information more than seven years old and bankruptcies more than 10 years old are examples of outdated information.
- Specific consent of the applicant is required for providing reports to the employer of the applicant.

iv. Fair Debt Collection Practices Act of 1978

This act is also used in conjunction with FCRA and it was amended in 2006.

Globally, there has been abundant evidence on use of abusive, deceptive and unfair debt collection practices by debt collectors.

Abusive debt collection practices are an invasion of privacy; this law was enacted specifically to address this issue.

Acquisition of location information:

Any debt collector, i.e., a credit card issuer communicating with any person other than the consumer for the purpose of obtaining location information (whereabouts such as address of the consumer, contact details, including mail address and telephone number) should not:

- State that the consumer owes any debt,
- Identify himself and state that he is confirming or correcting location information concerning the consumer, and, only if expressly requested, identify his employer,
- Ask for the information only once except under certain specific circumstances,
- In case of snail mail communication, provide an indication that the letter has originated from a debt collector,
- Contact the client directly when there is a Power of attorney except in exceptional situations.

Communication in connection with debt collection

- A debt collector, under normal circumstances, cannot meet the customer at any unusual time and/or unusual place, which would be inconvenient to the customer. A convenient time can be any time between 8 am and 9 pm.
- In case the consumer notifies that the he refuses to pay and wishes that there should be no further communication, the issuer would have to abide by that.

Harassment or abuse

- A debt collector may not engage in any conduct the natural consequence of which is to harass, oppress, or abuse any person in connection with the collection of a debt.

v. Credit Card Accountability Responsibility and Disclosure Act of 2009(CARD)

The Credit Cardholder's Bill of Rights Act 2008 could not be passed by the senate before the 110th session of the congress ended. Consequently, the rules were amended and renamed as the Credit Card Accountability Responsibility and Disclosure Act of 2009 or the Credit CARD Act of 2009.

This act was passed to amend the Truth in Lending Act and to establish fair and transparent practices relating to the extension of credit under an open-end consumer credit plan and for other purposes.

There are five titles to this act:

- Title I-Consumer Protection
- Title II-Enhanced Consumer Disclosures
- Title III-Protection of Young Consumers
- Title IV-Gift Cards
- Title V-Miscellaneous Provisions

Some highlights are as follows:

Prevents unfair increases in interest rates and changes in terms

- The issuer cannot increase the interest rate arbitrarily and it cannot be converted into default on existing balances universally;
- Interest rates on credit cards must be periodically reviewed by the credit card issuer and, if need be, decreased if indicated by the review.
- Credit card issuers cannot increase rates on a card during the first year of issue.
- If any promotional rates are offered, they must last at least six months.

Prohibits exorbitant and unnecessary fees

- Issuers cannot charge fees to pay credit card debt, whether by mail, telephone, or electronic transfer, except for live services to make expedited payments;
- Prohibits issuers from charging over-limit fees unless the cardholder elects to allow the issuer to complete over-limit transactions and limits over-limit fees on electing cardholders;
- Penalty fees charged by the issuer should be reasonable and proportional to the violation or omission by the card holder;
- Charges on low credit, high fee credit cards to be restricted.

Requires fairness in application and timing of card payments

- Payments in excess of the minimum balance should be first appropriated to the credit card balance with the highest rate of interest;
- Early morning deadlines for credit card payments cannot be adhered to by the issuer;
- All credit card statements must be mailed 21 days in advance before the bill is due.

Protects the rights of financially responsible credit card users

- Double cycle billing is banned. This implies that interest cannot be charged on debt paid on time;
- Late fees cannot be charged for delayed credit due to the issuer’s problem;
- In case the payment is made at local branches, it needs to be credited the same day;

- A consumer's ability to pay must be considered before issuing credit cards or increasing credit limits.

Provides enhanced disclosures of card terms and conditions

- Sufficient notice of not less than 45 days must be given to the card holder for interest rate fee and finance charge increases;
- At the time of renewal of the card, if terms and conditions have changed, they need to be communicated to the card holder;
- In case the card holder opts for minimum monthly payments, the total outflow period and total interest due as a result of minimum monthly payments need to be communicated to the card holder;
- The payment due dates and the applicable late payment penalties must be disclosed.

Strengthens oversight of credit card industry practices

- The credit card agreements should be available on the Internet and copies must be sent to the Federal Reserve Board, to enable them to post them on their Website;
- It is the responsibility of the Federal Reserve Board to review the consumer credit card market, including the terms of credit card agreements and practices of credit card issuers and cost and availability of credit to consumers;
- The Federal Trade Commission is vested with powers to make rules to prevent deceptive marketing of free credit reports.

Ensures adequate safeguards for young people

- A credit card cannot be issued to a person less than 21 years of age unless the application is signed by a parent or any other individual who is also older than 21 years. The parent or the individual will have to take the responsibility for the debt. Alternatively, the person less than 21 years needs to prove that he/she has independent means of repaying the debt;
- All limits extended to young customers' needs to be pre-screened;
- Increase in credit limits to young customers' needs to be approved by the parent or the other individual who is jointly liable for the same;
- Students must be protected against aggressive credit card marketing; it increases transparency of affinity arrangements between credit card companies and universities.

Enhanced penalties

- The penalties have been increased for companies that violate the Truth in Lending Act for credit card customers.

Gift card protections

- All gift cards must have at least an expiry of five years, eliminating the practice of declining values and hidden fees for those cards not used within a reasonable period of time.

Encourages transparency in credit card pricing

- The interchange fees disclosure, pricing and cost structure must be studied by the GAO.

Protects small businesses

- The use of credit cards by small businesses needs to be studied by the Federal Reserve and they need to make recommendations for administrative and legislative proposals;
- A Small Business Information Security Task Force to be established to address the information technology security needs of small businesses and help prevent the loss of credit card data.

Promotes financial literacy

Development of strategic plan to improve financial literacy education.

http://www.govtrack.us/congress/billtext.xpd?bill=h111-62)

8. Transactions on cards

a. Introduction

Transactions on cards form a major chunk in the entire life cycle of the cards.

They can be classified based on the mode of transactions.

They can happen in the following ways:

1) Card Present Transactions

- Point Of Sale Machine (POS)
- Automated Teller Machine (ATM)

2) Card Not Present Transactions

- Internet transaction
- Mobile transactions

b. Point of Sale Terminal (POS)

The largest channel through which transactions happen is POS. The POS machines are normally placed at the merchant location. Typically, POS machines will be provided by the acquirer. These machines can either be owned by the merchant or the acquirer.

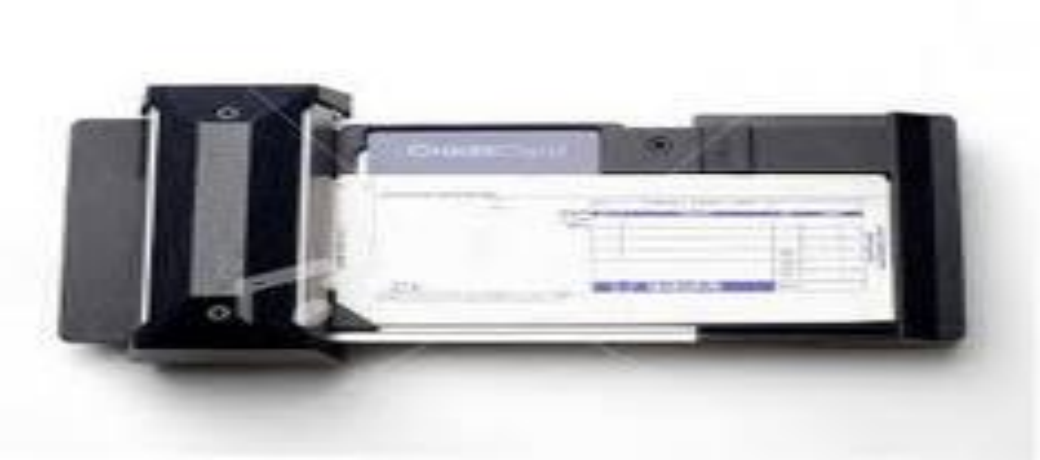
In case a merchant owns the machine, the cost of purchase will have to be borne by the merchant. In case the POS machine is owned by the acquirer, then the merchant has to bear a monthly rent. It makes business sense to lease out the POS machine rather than own the same. During the current period of intense competition, the monthly rentals model is also slowly becoming defunct.

Types of POS machine:

With changing card technology, the POS machines can either be manual, magnetic stripe-based or smart cards. Earlier, the POS machines were manual. The embossing on the cards was predominant in these days.

A typical manual swipe card machine is depicted below.

- The embossed card would be placed at the bottom of the machine.
- A charge slip is placed on top of it.
- On top of it is the lever-based machine, which will be run on the slip two to three times.
- On swiping the same, the embossed information will be reflected on the charge slip.
- The amount to be charged will be written on the slip by the merchant and then, authorization will be through a manual signature on the charge slip.



The merchant would check the authorization by verifying the signature on the charge slip with the signature on the panel at the back of the card. The merchant is also provided a hot listed booklet. The merchant has to ensure that the card to be processed is not in the hotlist. In the event of swiping a hot listed card, the onus would be on the merchant in the event of loss.

This manual system is only for credit cards and not debit cards.

Cards in the current era are not embossed. Non-embossed cards also have a caption, “Electronic Use” only. Electronic POS machines can be classified as Keyed POS or Swiped POS.

In a Keyed POS, a card number and expiry date are keyed in. This is generally done in cases where a card is not present in a transaction; it is more risky than a swipe card.

Swiped POS: Magnetic swipe cards follow a different technology. It applies to smart card POS as well. There are two types of smart card POS. One is contactless technology and the second is chip cards (with contact). There are three components of a POS Terminal: A magnetic stripe reader, a receipt printer, a key board and a modem. VeriFone is the market leader in POS Terminals. Technology has taken the POS Terminal to a different level - POS Systems. Users must not be confused with the POS Terminals. The POS system has a bigger connotation. The POS system can also be integrated into POS terminal. One model of the POS system can be seen in the retail store where the magnetic swipe is separate from the traditional POS machine.

Traditional POS Terminal

Standalone Card Reader

a. Smart Card Technology

Contactless cards/proximity cards do not require physical contact of the card with the reader. This type of card is very popular for public transport where the user need not take it out of the wallet. All the user has to do is just to show it in front of the reader. The technology being used in such cards is the Radio Frequency. It requires the card to be in proximity to an antenna to communicate. Contact Cards have an area which has to come into physical device for operating the card. Hybrid smart cards which have both contactless and contact option are also available.

EMV **(E**uropay **M**asterCard **V**isa) has created specifications that define the communication protocol between contactless card and merchant terminal. As already discussed in section 5, it is absolutely necessary for the interoperability of the cards, else the card becomes unusable. The current version of EMV standards is 4.2, released in June 2008. It also encompasses specifications, test procedures and compliance processes managed by EMV (www.emvco.com). It is not enough that the smart cards are EMV compliant. Devices like readers also need to be EMV compliant. Only then the two will work in tandem.

B. Connectivity

One of the critical success factors for electronic POS (for magnetic and smart cards) is the establishment of communication between merchants and acquirers. If connections are not established, it can come to a standstill. Hence, manual swipe becomes a back-up in the event of communication failure.

Communication channels between merchants and acquirers are as follows:

- PSTN (Normal Telephone lines-**P**ublic **S**witch **T**elephone **N**etwork)
- GPRS: New technology used for mobile is also used for wireless POS. Many petrol pumps use this technology as the device is mobile and the swiping happens in front of the customers.

- CDMA POS machines are also available in certain countries.
- Wi-Fi POS is also catching up.

c. Automated Teller machine (ATM)

Both debit and credit cards are used in ATMs for withdrawal of cash and operations on linked accounts.

The POS and the ATM technology, in terms of establishing a connection, are quite similar. The difference is the final process. Up to the point of authenticating the customer, it is the same. ATM is further bifurcated on the basis of magnetic and smart card readers. ATM, in terms of communication, requires a higher band width compared with a POS machine and one may not come across PSTN. The VSAT, leased lines and ISDN are the most popular modes of connectivity for ATMs.

ATM Business Models

There are bank owned as well as white label ATMs. In a white label ATM, the concept is similar to white label cards mentioned in an earlier section. In a white label ATM, the service provider owns it and billing happens based on the number of transactions. In a white label environment, the ATM will not have the name of any specific bank. The ATM displays the type of card it will accept (Visa, Mastercard, etc.). White label model is most popular in the US and Canada. Canada has more than 25% of ATMs in the white label environment. TNS Smart Network is the biggest white label ATM service provider in Canada with more than 13,000 ATMs. Some reputed ATM vendors are Diebold, NCR and Euronet.

Multi-Purpose ATM

ATMs have transformed from conventional cash dispensing machines to multipurpose utility ones. They can now be used for mobile top-ups, dispensing movie tickets, and topping up the public transport system. Singapore has a unique system of merging an ATM transaction and a public transport smart card.

The ATM will have two slots, one for cash withdrawal and the other for transport purposes. Both cards will be inserted simultaneously and using ATM cards, transport smart cards can be easily topped up. This has been modified further, with a single card currently being used as a smart card cum ATM card.

ATM Trends

One of the basic issues with ATMs is the cost of replacement. The smart card-based credit/debit cards are redefining ATM technology needs. The cost of replacing an ATM is much higher than that for replacing a POS terminal. To increase popularity and additional control, biometric ATMs are being introduced. A biometric ATM can either supplement the existing PIN mechanism or replace it. Replacing the PIN mechanism may have additional compensating control in terms of face recognition/IRIS scanner.

d. Internet Transactions

Use of credit cards on the Internet has become popular. Most of the shopping sites also accept credit/debit card transactions. Internet transactions are also classified as 'cards not present' transactions, since physical cards are not presented for debiting the same. The only authentication that used to happen on the credit card transactions on the Internet was the card number followed by the CVV2. The card and CVV2 can be easily stolen and transactions can be done easily. This has led to a second level of authentication. This code is referred to as VBV (**V**erified **b**y **V**isa) for the Visa and MSC (**M**asterCard **S**ecur**C**ode) for Master Cards. The secure code works similar to an ATM PIN. The code is given by the card issuer.

Certain issuers have two levels of secure code similar to banking. One is for query and the other one is for transaction. Citibank calls the former as Query Pin (QPIN) and the transaction one as (HPIN), specific to Internet transactions. Similarly, the merchant also needs to be registered to accept these secure codes. In certain geographies, the regulator can make the code mandatory. In the US, the registrations are not mandatory. The issuer can also define threshold amount beyond which this code becomes mandatory. The password syntax is also defined by the issuer.

Once registered, the VBV or MSC will display the personalized message of your name. This is a second-level check and only if the personal message is correct, the card holder should proceed with the entering the password. This is for protection of the card holder against fraudulent Internet merchants. The registration process for the secure code is simple. One can register independently or as a part of the purchase process. Both Visa and Mastercard allow registration at the time of purchase by answering a few simple questions.

In case of chip cards, card present transactions can be simulated by using secure code providing devices that use the card for generating a pin to be used.

e. Phone Transactions

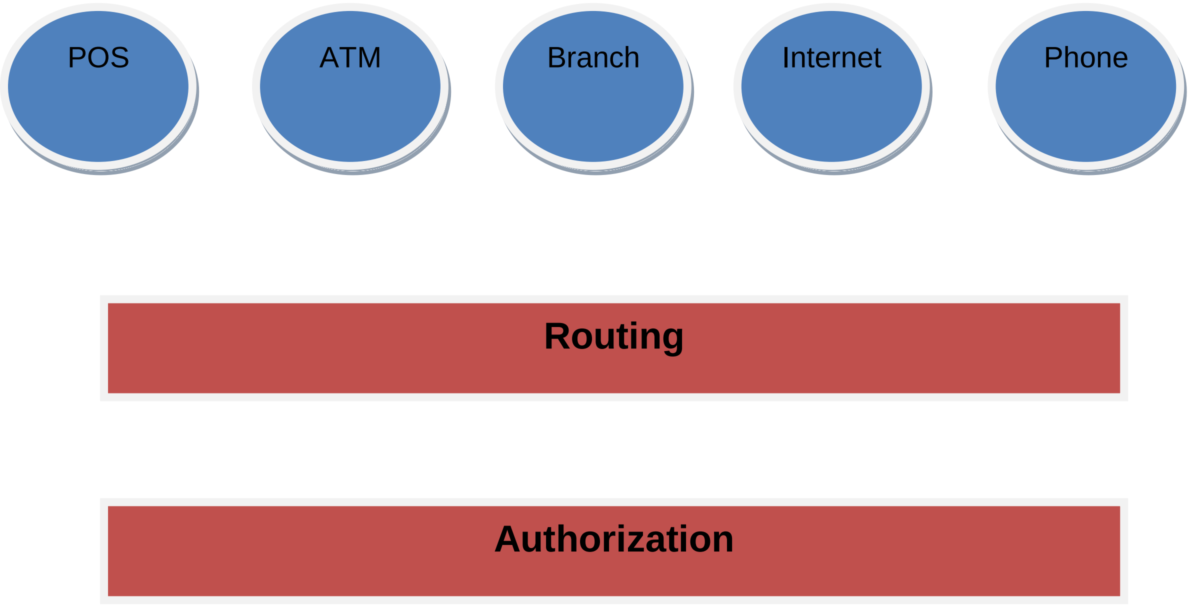
Card holders can undertake phone-based transactions and pay by card over phone as well. In such transactions, the CVV2 (also known as a three-digit security code) will be used for authentication purposes.

The card issuer can also have a T-Pin as additional authentication. The transaction over phone is classified as “card-not-present transaction”.

f. The switches

Switches form the back bone for POS, ATM and other channels; they are the most important layer in telecommunications. The basic function of a switch is to route transactions originated from a device to the issuer based on the attributes of the card.

In evolutionary stages, there were separate switches for separate devices such as POS switch, ATM switch etc. Now, switches are integrated. A schematic diagram is shown below:



One of the key issues with switches is OS and hardware compatibility.

American express and Visa are also going to provide network services between issuers and acquirers / gateways.

Popular switch providers:

In the payments industry, there are a number of names that one would come across.

Base 24 is one of the oldest names in the industry. It started as an ATM switch and now the company, ACI International, provides switches across various channels.

Opus is another company in the business of switches, in addition to a lot of other financial service products and solutions.

FIS Global is another switch provider.

BPC Smart Vista is a Russian company that offers a wide range of products besides switches.

Euronet started off with ATMs and it now operates a proprietary switch.

Venture Infotek (recently acquired by ATOS origin) is one of the leading POS switch providers in India.

g. Transaction Processing Cycle

The entire POS transaction has a transaction life cycle. The broad process cycle consists of:

- Authorization
- Batching
- Clearing
- Settlement

Batching, clearing and settlement will be discussed in subsequent sections.

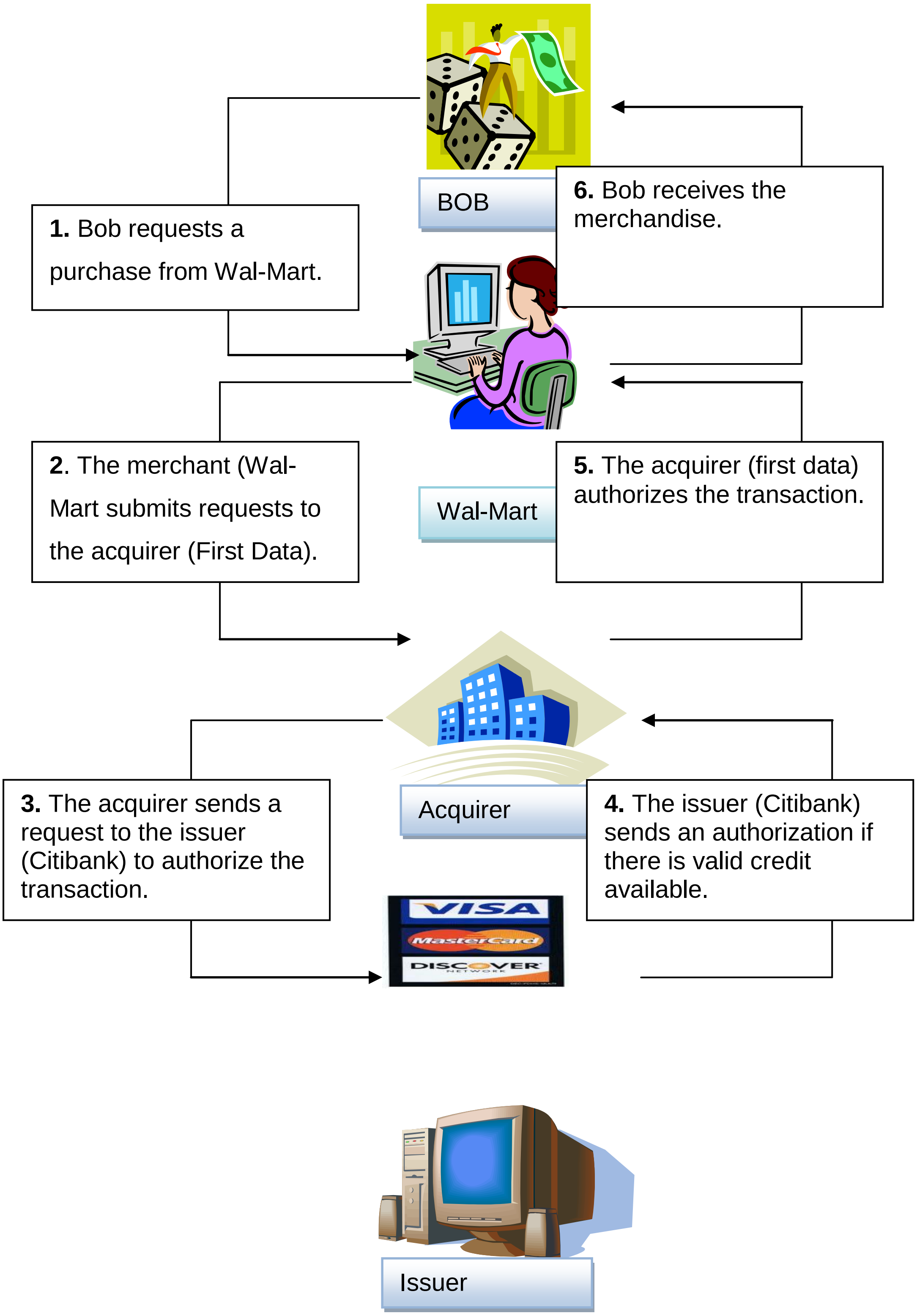
POS Authorization

In authorization, validation of credit limit happens. Prior to credit limit availability, authentication must happen. Authentication is a process where a client's credentials are established. In certain countries, even swiping of the credit/debit card requires a two factor authentication. It is not enough that the card is swept. Along with swiping, PIN also needs to be entered on the POS machine.

In a magnetic swipe card, the credentials are not stored on the card itself. The password and other details need to travel through the network for authentication purposes. In case of smart cards, password and other credentials are stored on the card and the reader is intelligent enough to do the authentication without the need for password and other credentials travelling through the network. The authentication mechanism in smart cards is stronger compared with magnetic strip cards.

Bob walks into Wal-Mart store in Chicago. He has a Visa Card issued by Citibank and Wal-Mart has POS machines of FirstData in its locations. Bob purchases merchandise worth $1500 from the store. The brief authorization cycle is depicted below. The authentication cycle is skipped in the flow.

Authorization Cycle



1. Bob requests a purchase from Wal-Mart.

2. The merchant (Wal-Mart submits requests to the acquirer (First Data).

3. The acquirer sends a request to the issuer (Citibank) to authorize the transaction.

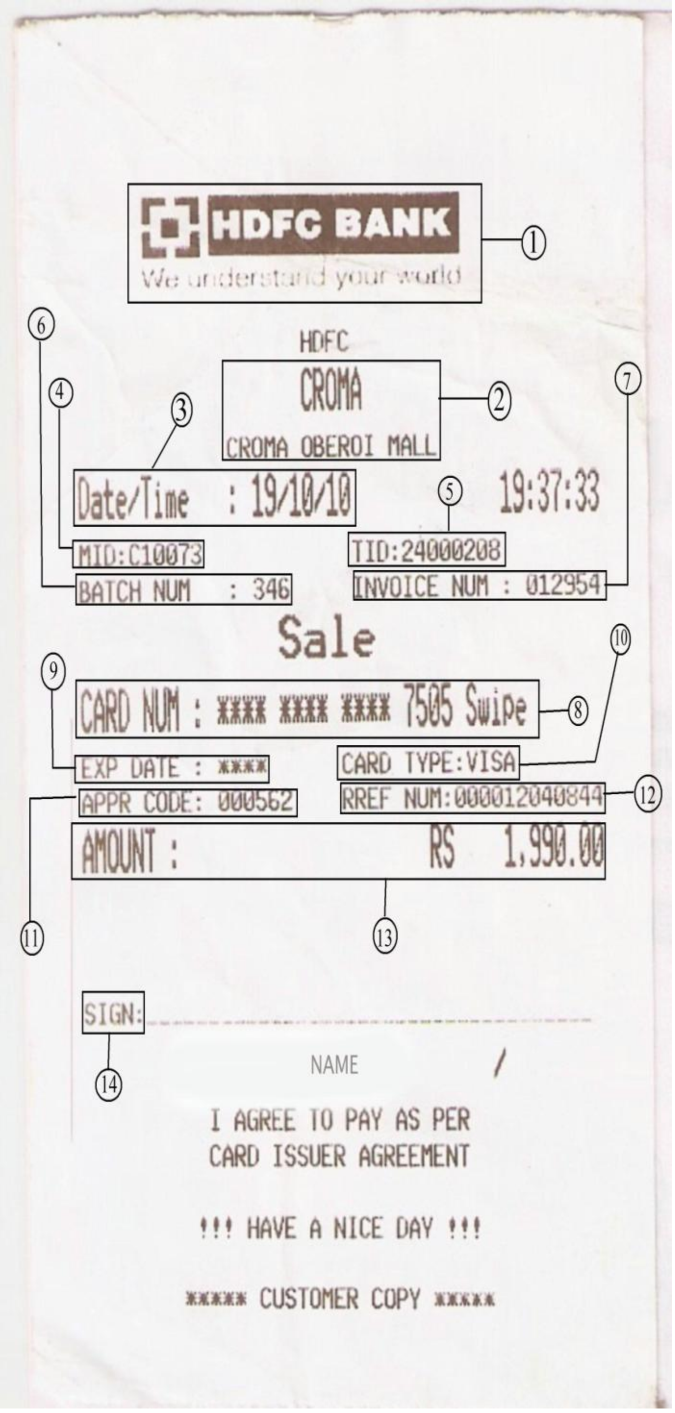
4. The issuer (Citibank) sends an authorization if there is valid credit available.

5. The acquirer (first data) authorizes the transaction.

6. Bob receives the merchandise.

An authorization slip will be generated on completion of the authorization process. If the transaction is not successful, it is termed as a declined transaction.

Authorization Slip



HDFC BANK
We understand your world

HDFC
CROMA
CROMA OBEROI MALL

Date/Time : 19/10/10 19:37:33
MID:C10073 TID:24000208
BATCH NUM : 346 INVOICE NUM : 012954

Sale

CARD NUM : **** **** **** 7505 Swipe
EXP DATE : **** CARD TYPE:VISA
APPR CODE: 000562 RREF NUM:000012040844
AMOUNT : RS 1,990.00

SIGN:
NAME /

I AGREE TO PAY AS PER
CARD ISSUER AGREEMENT

!!! HAVE A NICE DAY !!!

***** CUSTOMER COPY *****

1
2
3
4
5
6
7
8
9
10
11
12
13
14

Label	Description
1	Acquirer-HDFC Bank
2	Merchant Name-Croma
3	Date and Time of Transaction-19/10/10 19:37:33
4	Merchant ID(MID)
5	Terminal ID(TID)
6	Batch Number
7	Invoice number of the underlying transaction
8	Card number last 4 digits with the suffix Card reader mode
9	Expiry Date of the card which is masked
10	Card Type :Master/VISA/etc.
11	Approver Code:-mentioned in step 4 above
12	Transaction reference number
13	Approved amount
14	Signature of the Card holder. This signature must match the signature on the signature panel of the card
Generally, the authorization slip is printed in two copies. The first copy will be merchant copy and the second is card holder copy. The merchant copy will be sent to the acquirer at periodic rests.	

POS Transaction Routing

One of the important components in the authorization process is 'routing' of a transaction.

There are two types of transactions:

Sr No	Transaction Type	Example
1	On us	Example 1: The issuer and the acquirer are the same. Typically Amex works on this model. Example 2: Bob's card was issued by Citibank and the Wal-Mart acquirer is also Citibank.
2	Across network	The example discussed above is an 'across network'.

Let us assume that Bob uses the Visa card for the transaction. The most important point is that the merchant can connect directly to Visa's network (Visanet) for authentication. Wal-Mart can have a dedicated network of Visa i.e., all POS machines of Wal-Mart are connected directly to the Visa network without any other layer in between. Amex operates through this system. However, there are strings attached to the feasibility of connecting directly to the Visa network. One of the basic reasons is cost. It does not make business sense to opt for this unless there are minimum threshold transaction volumes.

Under certain circumstances, such as the issuer's system not being available, Visa may perform stand-in processing and review and authorize or deny the transaction.

The alternative to this is the use of a router/switch, which in turn will connect to the Visanet. The switches mentioned above based on the card BIN will route the transaction first to Visa and then to the respective issuer of Visa.

It also makes business sense to have a router/switch when the merchant is using multiple providers such as Master/Visa etc.

In case of international transactions, they can even hop three different switches.

All entities that connect to the Visa network (Visanet) through these switches are called Visa Net Processors (VNP). Details of VNP are discussed in section 9.

Transaction classification

Transactions on cards can be classified into various types; the classification is used for various purposes: settlement, identification, reporting etc. Visa has not less than 78 transaction types, of which the most popular ones are discussed below.

Classification 1:

Card Present Transaction vs. Card Not Present

When a card is swiped or brought into contact with the POS/ATM, the transaction is classified as transaction present.

When a client places an order for buying through the Internet or a MOTO (Mail Order/Telephone Order), it will be treated as a card not present transaction. If a POS machine uses a keyed data, then also it will be treated as a card not present transaction.

An electronic transaction must be identifiable at the authorization stage as well as the clearing record level.

Classification 2:

NSR Transaction:

No **S**lip **R**equired (NSR) transaction is a category, where the transaction slip need not be generated. This is controlled at the Merchant Category Level (MIC). For example, MIC 5499-Convenience store is an example of NSR transaction. However, the value of a transaction should also be below a threshold level. Typically, an NCR will also be applicable to small-ticket transactions.

In case of dynamic currency conversion on a transaction, it cannot be processed as an NSR even though it is a small-ticket transaction.

Small Ticket Transaction:

A transaction having a value of less than $25/GBP10 is defined as a small ticket transaction subject to the following:

- Be conducted in a face-to-face environment
- Be authorized
- Have a POS entry mode code value
- For magnetic stripe cards only specific MCC can enter into a small-ticket transactions
- For contactless chip cards and proximity payment devices, there is no restriction of MCC.

Classification 3:

This classification is based on the merchandise or services rendered.

Transaction type	Transaction description
Installment billing transactions	The card holder buys merchandise and agrees to pay for it in installments. This is similar to EMI on loans.
Advance deposit transactions	A transaction that a hotel or cruise line completes, resulting from a Visa cardholder's agreement to use a Visa Card for payment of an advance deposit to reserve accommodations.
Delayed delivery	A single transaction where a card holder completes two separate transaction receipts. The first Transaction Receipt functions as a deposit (such as a down payment) for goods or services; the second is to pay the balance due the Merchant A delayed delivery transaction is one where the delivery of the merchandise happens at a later date. A merchant in USA must obtain separate authorization for the deposit and final payment .The receipt must have the indication in writing as " Delayed Delivery", "Deposit" or " Balance"
Bill Payment Transaction	Utility payments such as mobile, electricity and other utilities can be paid using credit cards. All such payments will be categorized as bill payment transactions. These may be recurring / scheduled in advance.

Classification 4:

Dynamic Currency Conversion (DCC)

Generally, the currency of all transactions accepted at the point of transaction is the local currency of the transaction country. However, there can be situations where transactions need to be undertaken in the currency of the card issuer. The conversion of purchase price of goods or services from one currency to another is as agreed to by the card holder and merchant. This currency becomes the transaction currency, regardless of the merchant's local currency. All merchants and acquirers cannot offer dynamic currency conversion unless they are registered with Visa. Heavy penalties are imposed on merchants that undertake a dynamic currency transaction without the necessary approvals. The conversion is made based on daily FX rates.

Classification 5:

Credit Transaction: This type of transaction is very popular in the airlines when a passenger books a ticket and subsequently cancels it. Similarly, in the US, when a card holder returns the defective merchandise within a pre-specified period, the credit transaction receipt must specifically mention the merchandise returned, services cancelled or adjustments made. In case of airline cancellations, receipts are not mandated. The merchandise return policy needs to be clearly defined by the merchant.

Transaction Reversal: The merchant can process a reversal or an adjustment within 30 days if it processed as a Transaction Receipt in Error. This must happen using a specific reversal transaction code.

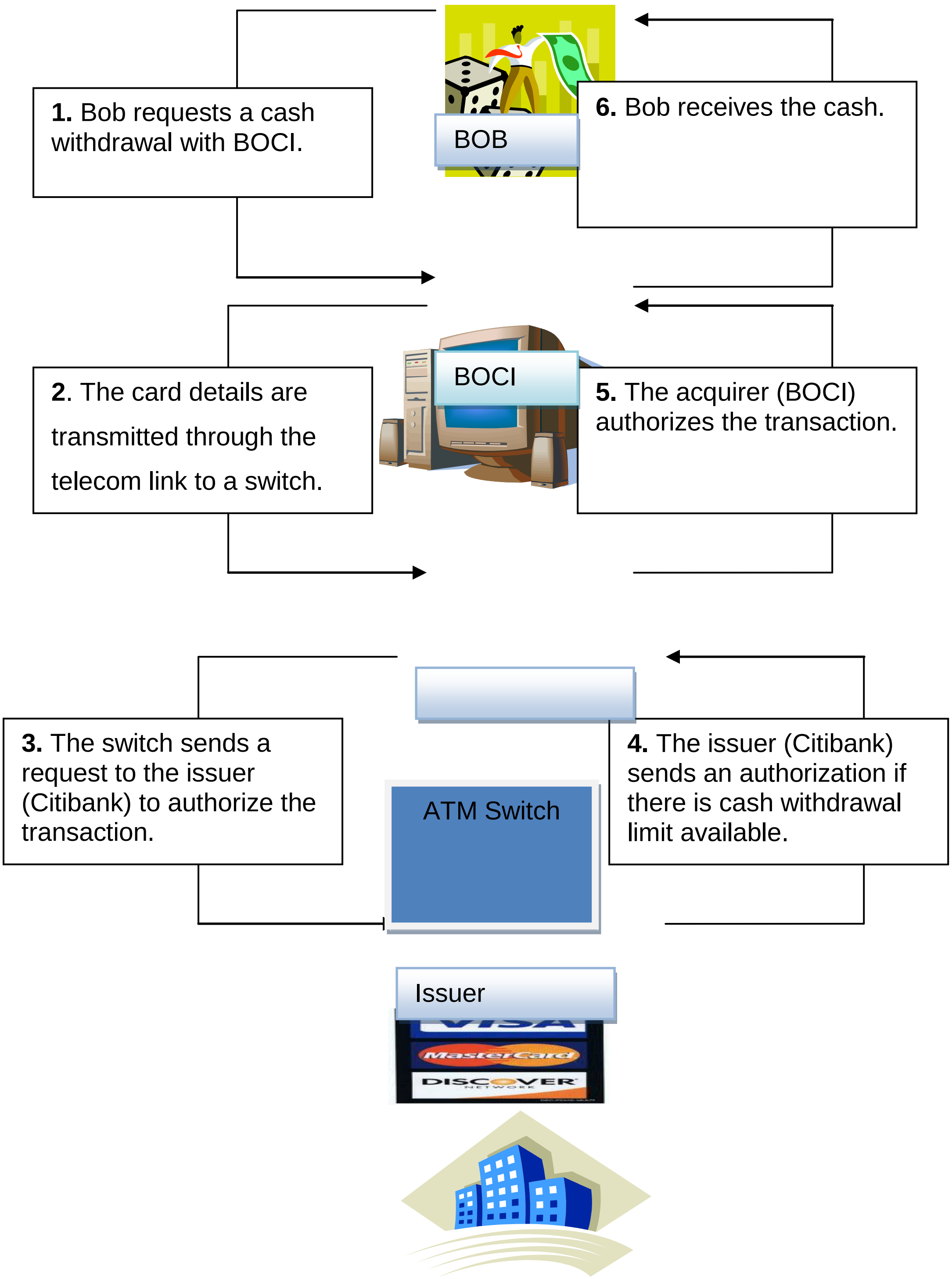
The former is a genuine reversal where the client returns the merchandise or service while the latter is an error or omission at the merchant's end.

ATM Authorization

The ATM authorization process is also similar to POS authorization except in few aspects.

The flow of ATM is as follows:

Bob walks into a BOCI (Bank of California International) ATM in Chicago. His credit card is issued by Citibank.



1. Bob requests a cash withdrawal with BOCI.

2. The card details are transmitted through the telecom link to a switch.

3. The switch sends a request to the issuer (Citibank) to authorize the transaction.

4. The issuer (Citibank) sends an authorization if there is cash withdrawal limit available.

5. The acquirer (BOCI) authorizes the transaction.

6. Bob receives the cash.

9. Card Security

a. Introduction

In the current era, with information explosion all around, fraud such as identity theft is can be committed easily. Fraud and identity theft have far-reaching consequences on the financial services industry.

One of the most susceptible segments of financial services is the cards industry. Card level security has been evolving over the years. The transformation from magnetic stripe cards to smart cards was more due to security concerns rather than convenience. Since Sep 2010, Canada has moved to smart cards completely. Nonetheless, smart cards are also vulnerable. When a product is new, the inherent risks are high and only over a period of time can new risks be identified and mitigated.

PCI-DSS (**P**ayment **C**ard **I**ndustry-**D**ata **S**ecurity **S**tandard) was the brain child of PCI Security Standards Council which is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

The organization was founded by American Express, Discover Financial Services, JCB International, Master Card worldwide and Visa Inc in 2006. The mission of PCI Security Standard Council is to enhance payment account data by driving education and awareness of the PCI Security Standards.

The PCI Security Standards Council has until date come out with three standards:

- PCI-DSS
- PTS-Pin Transaction Security Standard
- PA-DSS-Payment Application Data Security Standard.

b. PCI-DSS

Background

The current version of the standard is 1.2.1, with effect from July 2009. The standard includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. The ultimate objective is to proactively protect customer account data. **The 2.0 version of the standard is expected in Q1 2011.**

The PCI DSS is not a self-assessment where the responsible person certifies that the organization has adhered to PCI-DSS. The PCI SSC (**S**ecurity **S**tandard **C**ouncil) has authorized certain organizations to validate an entity's adherence to PCI-DSS. These authorized organizations are referred to as "Qualified Security Assessors" or "QSAs". The QSAs have to demonstrate the necessary competence related to the knowledge and the ability to undertake validation assessments.

There are detailed procedures to be adhered to by the QSAs.

The two parties who need to adhere to the PCI DSS are:

- Merchants
- Service providers

Approved Assessors

PCI–DSS has to approve the QSA. The following segments also need to be registered for PCI-SSC:

- ASV (Approved Scanning Vendors): They are organizations that validate adherence to certain DSS requirements by performing vulnerability scans of Internet facing environments of merchants and service providers.
- PA-QSAs are Payment Application Qualified Security Assessors (PA-QSAs). They validate the Payment Application.

i. P C I-DSS overview

The PCI-DSS is a consolidated document. There are six principles on which this standard is built and within these principles, 12 are embedded requirements.

No	Principle
1	Build and maintain a secure network
2	Protect card holder data
3	Maintain a vulnerability management program
4	Implement strong access control measures
5	Regularly monitor and test network
6	Maintain an information security policy

The PCI–DSS requirements are applicable only if the Primary Account Number (PAN) is stored, processed or transmitted. If it is not stored, processed or transmitted, then these guidelines do not apply.

A sample grid of various data elements with regard to storage and protection is provided below:

	Data Element	Storage Permitted	Protection Required	PCI DSS Req-3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Card Holder Name	Yes	Yes	No
	Service Code	Yes	Yes	No
	Expiration Date	Yes	Yes	No
Sensitive Authentication Data	Full Magnetic Stripe Data	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN /PIN Block	No	N/A	N/A

It is important to note that both merchants and service providers have to undergo PCI-DSS. The sensitive authentication data must not be stored after authorization even if it is encrypted. The scope of PCI-DSS Compliance assessment is applicable to all the system components, which are any network components, servers or applications that are included in or connected to the cardholder data environment. A card holder environment is that part of the network that possesses card holder data or sensitive authentication data.

Network components include, but are not limited to, firewalls, switches, routers, network appliances, wireless access points and other security appliances. In case wireless technology is being used at the POS or the server side for LAN Connection in the card holder environment, the PCI DSS requirements will have to be looked into. An organization must undertake risk assessment prior to implementation of wireless technology.

Server components include web server, application server, databases, operating systems, mail servers, proxy servers, authentication servers such as RADIUS, Network time protocol (NTP) and Domain Name servers (DNS). Applications include purchased and custom including internal and external applications. In the event the service provider or the merchant outsources any of its activities, it has a material impact on the assessment. The third party is also subject to PCI DSS compliance.

The PCI DSS Compliance of a third party can be handled in two ways:

- The third party itself is a PCI DSS complaint organization
- The services will be reviewed by the principal as a part of its PCI DSS compliance.

Business facilities also must be part of PCI DSS compliance. Business facilities will include stores, corporate offices, and franchise merchants.

Build and maintain a secure network (https://www.pcisecuritystandards.org)

There are two requirements under this principle:

Requirement 1	Install and maintain a firewall configuration to protect card holder data.
Requirement 2	Do not use vendor supplied defaults for system password and other security parameters.

Within each requirement, there are sections and sub-sections.

Section	Section Heading	No of sub sections
1.1	Establish fire walls and router configuration standards	6
1.2	Build a firewall configuration that restricts connection between distrusted networks and any system components in the card holder environment	3
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment	8
1.4	Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet	0
2.1	Always change vendor-supplied defaults before installing a system on the network	1
2.2	Develop configuration standards for all system components	4
2.3	Encrypt all non-console administrative access	0
2.4	Shared hosting providers must protect each entity's hosted environment and card holder data	0

Protect card holder data

Requirement 3	Protect stored card holder data
Requirement 4	Encrypt transmission of card holder data across open public network

Details of various sections and sub-sections are as follows:

Section	Section Heading	No of sub sections
3.1	Keep card holder data storage to minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to what is required for business, legal, and/or regulatory purposes, as documented in the data retention policy	0
3.2	Do not store sensitive authentication data even if it is encrypted	3
3.3	Mask PAN when displayed (The first six and last four digits are the maximum number of digits to be displayed)	0
3.4	Render PAN at minimum unreadable anywhere it is stored	1
3.5	Protect cryptographic keys used for encryption of card holder data against disclosure as well as misuse	2
3.6	Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of card holder data	8

Maintain a vulnerability management program

Requirement 5	Use and regularly update anti-virus software or programs
Requirement 6	Develop and maintain secure systems and applications

The details of various sections and sub-sections are as follows:

Section	Section Heading	No of sub sections
5.1	Deploy anti-virus software on all systems commonly affected by malicious software	1
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs	0
6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	0
6.2	Establish a process to identify newly discovered security vulnerabilities. Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.	0
6.3	Develop software applications in accordance with PCI DSS based on industry best practices and incorporate information security throughout the software development life cycle.	7
6.4	Follow change control procedures for all changes to system components.	4
6.5	Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in	10

	software development processes.	
6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks.	0

Implement strong access control measure

Requirement 7	Restrict access to card holder data by business need to know
Requirement 8	Assign a unique ID to each person with computer access
R9quirement 9	Restrict physical access to card holder data

Details of the various sections and sub-sections are as follows:

Section	Section Heading	No of sub-sections
7.1	Limit access to system components and card holder data to only those individuals whose jobs require such access.	4
7.2	Establish access control for systems components with multiple users that restricts access based on a user's need-to-know and is set to 'deny all' unless specifically allowed.	3
8.1	Assign all users a unique ID before allowing them to access system components or card holder data.	0
8.2	In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: • Password or passphrase • Two-factor authentication	0

8.3	Incorporate two-factor authentication for remote access to network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller, access control system (TACACS) with tokens; or VPN with individual certificates.	0
8.4	Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	0
8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components.	16
9.1	Use appropriate facility controls to limit and monitor physical access to systems in the card holder data environment.	3
9.2	Develop procedures to help all personnel easily. Distinguish between employees and visitors, especially in areas where cardholder data is accessible.	0
9.3	Make sure all visitors are handled well.	3
9.4	Use a visitor log to maintain a physical audit-trial of visitor activity. Document the visitor’s name, firm represented, and the employee authorizing physical access on the log. Retain this log for a minimum of three months, unless restricted by the law.	0
9.5	Store media back-ups in a secure location, preferably an	0

	off-site facility, such as an alternate or back-up site or a commercial storage facility. Review the location's security at least annually.	
9.6	Physically secure all paper and electronic media that contains cardholder data.	0
9.7	Maintain strict control over internal or external distribution of any kind of media that contains card holder data.	2
9.9	Maintain strict control over storage and accessibility of media that contains card holder data.	0
9.10	Destroy media containing card holder data when it is no longer needed for business or legal reasons.	2

Regularly monitor and test network

Requirement 10	Track and monitor all access to network resources and card holder data.
Requirement 11	Regularly test security systems and processes.

Section	Section Heading	No of sub sections
10.1	Establish a process for linking access to all system components to each individual user.	0
10.2	Implement automated audit-trials for all system components to reconstruct events.	7
10.3	Record audit trial entries for all system components for each event.	6

10.4	Synchronize all critical system clocks and times.	0
10.5	Secure audit trails so that they cannot be altered.	5
10.6	Review logs for all system components at least daily. Log reviews must include those servers that perform security functions such as intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers.	0
10.7	Retain audit trial history for at least a year with a minimum of three months immediately available for analysis.	0
11.1	Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.	0
11.2	Run internal and external network vulnerability scans quarterly and after any significant change in the network.	0
11.3	Perform internal and external penetration testing at least once a year and after any significant infrastructure or application upgrade or modification.	2
11.4	Use intrusion-detection systems, and/or intrusion-prevention to monitor all traffic in the card holder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and intrusion-prevention engines up-to-date.	0
11.5	Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system	0

	files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	

Maintain an information security policy

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

The relevant sections and sub sections are as follows:

Section	Section Heading	No of sub sections
12.1	Establish, publish, maintain and disseminate a security policy.	3
12.2	Develop daily operational security procedures that are consistent with requirements in this specification.	0
12.3	Develop usage policies for critical employee-facing technologies to define proper use of these technologies for all employees and contractors.	10
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	0
12.5	Assign to an individual or team, the information security management responsibilities.	5
12.6	Implement a formal security awareness program to make all employees aware of the importance of card holder data security.	2

12.7	Screen potential employees prior to hiring them to minimize the risk of attacks from internal sources.	0
12.8	If card holder data is shared with service providers, maintain and implement policies and procedures to manage service providers.	4
12.9	Implement an incident response plan. Be prepared to respond immediately to a system breach.	6

ii. Visa Net Processors (VNP)

Processors, member financial institutions or merchants are directly connected to Visa's proprietary network for transaction authorization. The switches discussed earlier will come under the category of VNP, which also has to undergo the PCI-DSS compliance. Any entity that is connected to Visa via Visanet Extended Access Server (VEAS) is a Visa Net processor. So an acquirer or an issuer who connects directly too will be categorized as a VNP.

iii. Pin Transaction Security (PTS)

The version 3.0 of PTS was launched in May 2010. Unlike PCI DSS, there are a number of independent documents for these PTS Security requirements:

- PTS security document
- Listing of approved devices
- Derived test requirements for vendors; Devices covered here are:

  - PCI Encrypting PIN Pad (EPP)
  - PCI POS PIN Entry Device (PED)

   - PCI Unattended Payment Terminal (UPT)
   - PCI Hardware Security Module (HSM))
- Questionnaire with updated criteria for vendors to fill and submit to labs.

iv. PA-DSS

PA-DSS (Payment Application-Data Security Standard) is derived from PC-DSS. The current version v1.2.1 is in use. The application scope is different in case of PA-DSS. PCI-DSS is applicable to merchants and service providers whereas PA-DSS is applicable to software vendors and others who develop payment applications that store, process or transmit card holder data as a part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties.

The structure of this document follows the PCI-DSS structure. There are 14 requirements of PA-DSS:

Requirement	**Description**	**Mapping to PCI-DSS**
1	Do not retain full magnetic stripe, card validation code or value (CAV2,CID,CVC2,CVV2) or PIN block data	3.2
2	Protect stored card holder data	3.1
3	Provide secure authentication feature	8.1,8.2 and 8.5.8-8.5.15
4	Log payment application activity	10.1,10.2
5	Develop secure payment applications	6.3,6.5
6	Protect wireless transmissions	1.2.3 & 2.1.1
7	Test payment applications to address vulnerabilities	6.2

8	Facilitate secure network implementation	1,3,4,5 and 6.6
9	Card holder data must never be stored on a server connected to the Internet	1.3.2
10	Facilitate secure remote software updates	1,12.3.9
11	Facilitate secure remote access to payment application	8.3
12	Encrypt sensitive traffic over public networks	4.1,4.2
13	Encrypt all non-console administrative access	2.3
14	Maintain instructional documentation and training program for customers, resellers, integrators	N/A

c. Transaction Processing

I. Introduction

Transaction processing is the backbone of the card process lifecycle. Processing has a number of stages. The entire POS transaction has a transaction life cycle. The broad process cycle consists of:

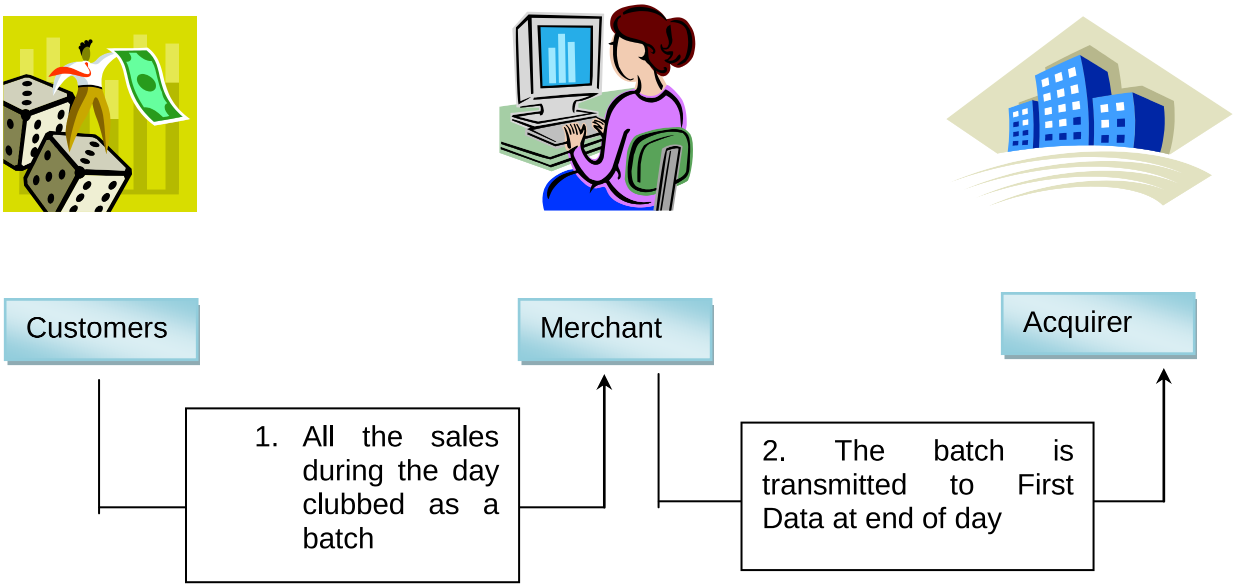
- Authorization
- Batching
- Clearing
- Funding

Authorization of POS, ATM, Internet and telephone, and mobile phone mounted chip cards has already been discussed in depth. . Another set of transactions comprise standing instructions such as periodic debit of mobile bill and other utility payments to the card account. These types of transactions do not have authorization (have one-time authorization) and are also clubbed under “Card Not present Transaction” similar to the Internet and telephonic transactions.

II. Batching

Batching is the second step in the transaction life cycle. At the end of the day, the merchant reviews sales through the day to ensure they were authorized and signed by card holders. The merchant then transmits all sales at once, called a batch, to the acquirer to receive payment. Extending the example of authorization of BOB, the related parties are as follows:

Participant	Details
Card Holder	BOB
Merchant	Wal-Mart
Acquirer	First Data
Issuer	Citi Bank
Card Network	VISA


Customers
Merchant
Acquirer
1. All the sales during the day clubbed as a batch
2. The batch is transmitted to First Data at end of day

In the HDFC charge slip in section 8, the label number 6 pertains to the batch number. The merchant will club the transaction under batch 346 for the day. All charge slips (also known as transaction deposits), where the customer has authorized, will also be bundled together and sent to the acquirer, i.e., First Data. The VISA international operating guidelines have laid down the following guidelines for transaction deposits.

III. Transaction Slip Deposit

For card present transactions captured through a POS/ATM or otherwise, slips of the transactions need to be deposited within the timeline stipulated by Visa. There will be no deposit of NSR (No Slip Required) and small-ticket transactions.

Transactions have been classified as:

Transaction Type	Transaction Deposit Guidelines in the US (which is different from other geographies).
T&E (travel and entertainment)	Three calendar days from transaction date, either to the acquirer or its agent.
Installment Billing transactions	The first billing installment transaction can be deposited only after the shipment of goods. The merchant must deposit subsequent installment billing transactions after 30 calendar days or on the monthly anniversary of the shipping date.
Delayed Delivery Transaction	Five calendar days from the date of deposit and final payment.
Multiple Merchant Outlets	Companies such as Wal-Mart can decide that all transactions across their outlets can be centralized for business and control purposes. Under such circumstances, transaction slips have to travel from branches to their centralized operations and then to acquirers. This is not possible in a short span of three days and hence, they have different deadlines. • Transaction receipt within 15 calendar days

	• Credit Transaction Receipts within five calendar days

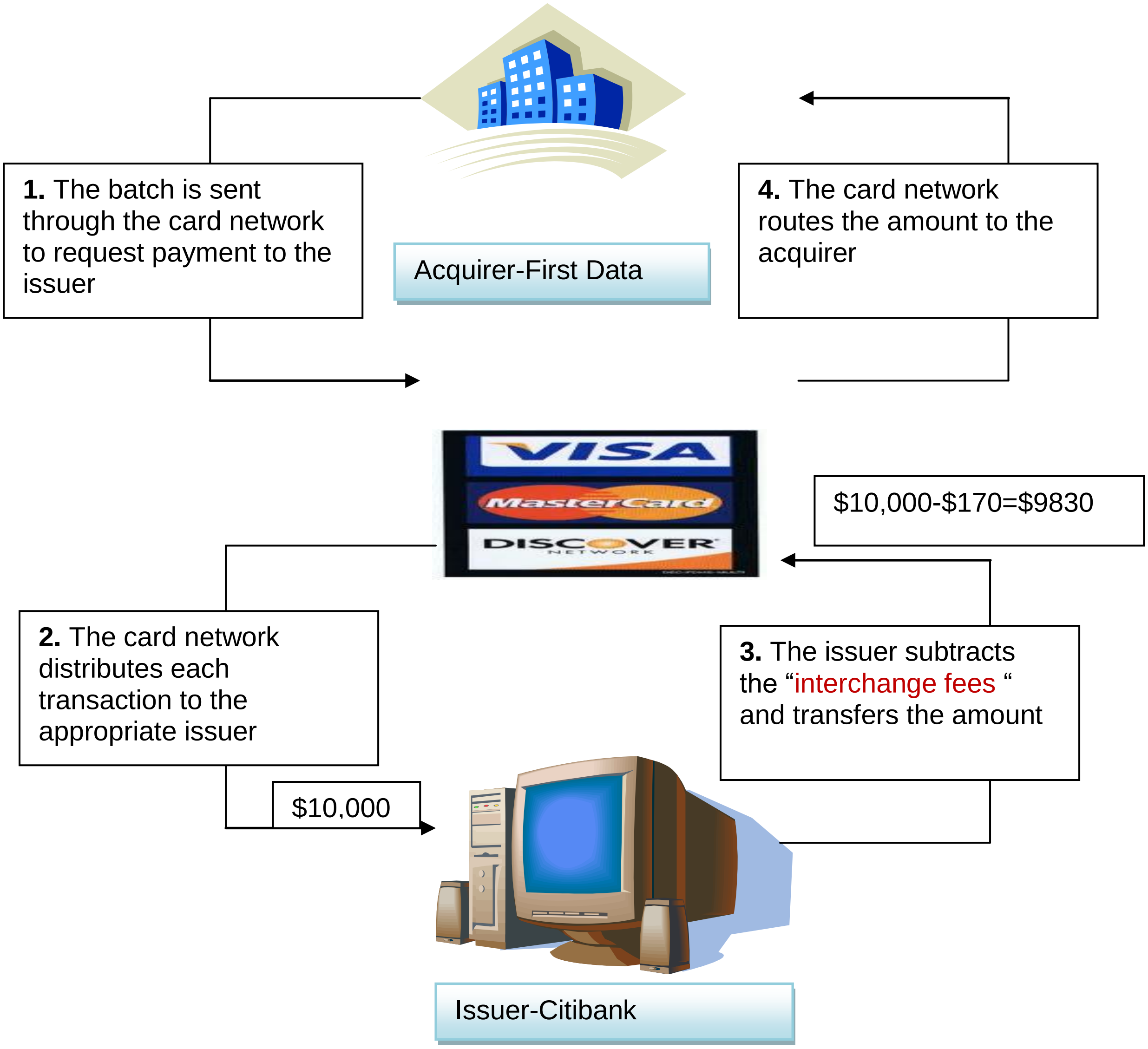
- All transactions should be deposited by a merchant, except a military base or an international travel agency, in the transaction country.
- All deposits should be made within three business days of the transaction date (two days for Visa Electron Cards).

Let us assume that the batch number for the transaction submitted by Wal-Mart is 346 and the total amount under that batch is $10,000

IV. Clearing

The next step in the transaction processing cycle is clearing. Once the acquirer receives the batch, it sends it through the card network, where each sale is routed to the appropriate issuing bank. The issuing bank then subtracts interchange fees, which are shared with the card network, and transfers the remaining amount through the network, back to the acquirer.

Clearing Cycle



1. The batch is sent through the card network to request payment to the issuer

Acquirer-First Data

4. The card network routes the amount to the acquirer

$10,000-$170=$9830

2. The card network distributes each transaction to the appropriate issuer

3. The issuer subtracts the "interchange fees " and transfers the amount

$10,000

Issuer-Citibank

Clearing is not as simple as it sounds. This process will aggregate all transactions at the issuer level, subtract the fees, and arrive at the amount. It will have credit transactions as well. In case of dynamic currency conversion, the amount is converted to appropriate settlement currency.

Clearing statement - Local currency transactions for batches

Acquirer ⇨	First Data	Global Payments	Heartland Payment Systems
Issuer-Citibank			
Gross transaction amount	$1600	$2000	$1500
Credit transactions	-	-$60	-
Transaction reversals			-$10
Charge backs	-	-	-
Interchange Fees	-$32	-$35	-$35
Net amount to be paid	**$1568**	**$1905**	**$1455**

The above example is for illustration purposes only to conceptually understand various components of clearing. Complexities are compounded as issuers are also acquirers for others.

This is further complicated by multiple currency transactions and multiple products within Visa itself.

Bob goes to Australia and purchases merchandise worth AUD150 (Australian Dollars). His card was International Visa card issued by Citibank, New York. Under normal circumstances (ignoring a dynamic currency conversion transaction), the merchant will have to receive the amount in AUD, which is the transaction currency, while Bob will be billed in USD. So, the value of Bob's purchase in AUD must be converted into USD. This is referred to as currency conversion.

A currency conversion rate will be either:

- A rate selected by Visa from the range of rates available in wholesale currency markets on the applicable central processing date plus or minus any adjustment determined by the issuer **OR**
- The government mandated rate in effect on the applicable central processing date, plus or minus any adjustment determined by the issuer.

In certain cases, the conversion rate will not be immediately known at the time of authorization. So, for the purpose of marking a hold in the credit card account and to arrive at available limit, the issuer may apply an ad hoc conversion rate. But at the time of final posting of transactions in client accounts, rates will be different. In case of debit card or an ATM transaction, amount will be posted in the client account instantaneously. Any adjustment at the time of clearing will result in a separate debit or credit transaction as the case may be. This will happen for each issuer and statement. At this juncture, no movement of funds will take place between any parties. The clearing process only arrives at the monetary amount, which each issuer has to pay to the acquirer.

Real-Time Clearing of Visa Debit Cards:

In a normal process, at the time of authorization of a transaction, a necessary hold will be placed in the account for the transaction and the withdrawal limit is reduced. Let us assume that Peter has a balance of $100 in his checking account with Well's Fargo and his debit card is linked to the Well's Fargo account. He swipes his card for $20 at a consumer store on 1st October 2010. As a part of authorization process, the gas station can place a hold for more than $20 as a market practice (Say $50 in this case). User may be confused as to how $50 is blocked for a purchase of $20.

Pre-Authorization

The Gas station POS has different business logic compared with normal authorization requests. In gas stations in the US, terminals are programmed to confirm that one has sufficient available balance to pay for average purchase of gas. Before pumping of gas, a pre-authorization request will be sent by the terminal. The amount in the pre-authorization request based on the spending pattern for Peter may be $50. The issuer can decide the maximum limit for pre-authorization request transactions.

Another popular use of pre-authorization request is in case of hotel payments. Peter walks into a hotel where the tariff is $30 a day and he intends to stay for three days. The exact liability of Peter to be paid to the hotel will be known at the end of day three as he may or may not use all the facilities. At the same time, the hotel may want to secure the payment. It will request Peter for his card and based on approximate spending, say $50 per day for three days, the hotel will send a pre-authorization request to the issuer for $150. This will result in a hold in his account for the next three days until he checks out. On the third day, when Peter checks out, his actual bill comes to $145. At that point, when the card is swept for the second time, the pre-authorization hold will be released and the $145 transaction will be executed.

The hold will be released only after the transaction of $20 is cleared and settled in the system. This actually leads to the customer being inconvenienced for $30, which is blocked and cannot be utilized until the settlement process is complete.

This is now obviated by a new process called Real-Time Clearing System, under which the hold needs to be released within the time stipulated in pre-authorization request. As a result, the customer account will be debited within the stipulated period of two hours from the transaction. Currently, the transaction limit is $500. This was initially introduced for gas stations, and effective Oct 2009, it was extended to super markets, quick service restaurants, bill payment services and department stores.

V. Settlement

Settlement is a process where actual movement of funds happens from the issuer to the acquiree through the Visa Net and finally to the merchant account. There can be multiple legs in the settlement process.

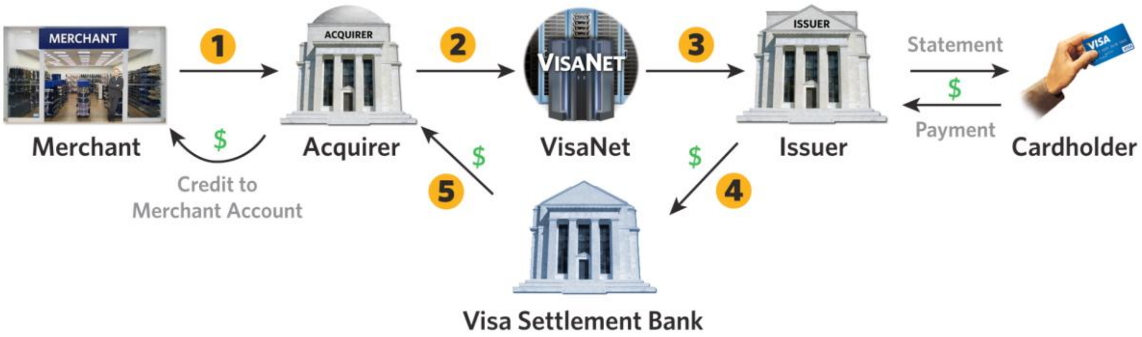
There is a critical role of the settlement banker in the entire process. Continuing the clearing example:

Transaction Leg	Transaction Nature
Leg 1	Citibank as an issuer has to pay $4928 ($1568+$1905+$1455) to Visa. The Citibank account will obviously be with Citibank. There will be a designated account for the same (Citi Card account). The amount will be paid to the Visa Settlement Account.
Leg 2	Visa Settlement account (which is a bank account) is credited by $4928. There can be two scenarios: **Scenario 1:** Visa settlement account is also with Citibank. In that case, the process is simpler called internal transfer where the Citi card account is debited and the Visa settlement account is credited. **Scenario 2:** Visa settlement account is with Wells Fargo In this situation;

	Citibank has to request the bank branch with which it holds the Citi Card account to transfer the proceeds to Wells Fargo. This will happen through the Federal Reserve's National Payment System.
Leg 3	Visa settlement account would be debited (assuming scenario 2) for $4928.
Leg 4	➢ First Data's settlement account is credited $1568 through internal transfer if First data's settlement account is also with Wells Fargo; otherwise it happens through the Federal Reserve's National Payment System. ➢ Global Payment's settlement account is credited $1905 through internal transfer if Global Payment's settlement account is also with Wells Fargo; otherwise it happens through the Federal Reserve's National Payment System. ➢ Credit Heartland Payment System's settlement account is credited $1455 through internal transfer if Global Payment's settlement account is also with Wells Fargo; otherwise it happens through the Federal Reserve's National Payment System.
Leg 5	➢ First Data has to credit the respective merchant accounts that had done these transactions. There can be number of merchants behind these transactions. Similarly, Global Payment settlement will also have to credit the respective merchant account. ➢ Similarly Heartland Payments also will have to credit the respective merchant account.

The settlement account and merchant account are special types of accounts of the acquirers and merchants. They do not have the checking facility in this account.

The entire clearing and settlement process is summarized schematically:



Courtesy: Visa-international-operating regulations core

1, 2 and 3 happens on T day while 4 and 5 on T + 1 day

VI. Charge backs

Charge back is a process where a transaction disputed by the card holder is reversed and the amount is recovered from the merchant by the issuer. There is a subtle difference between a credit transaction and a charge back. In a credit transaction, the card holder approaches the merchant who initiates the credit transaction and the same is routed through an acquirer.

In a charge-back, the issuer initiates the transaction. There is no authorization required from the acquirer or the merchant for a charge-back. Necessary checks and balances have to be built into the system; for the same transaction, the card holder is credited via credit transaction as well as a charge-back for the same. Charge backs to the acquirer can be disputes; dispute resolution is a four-step process.

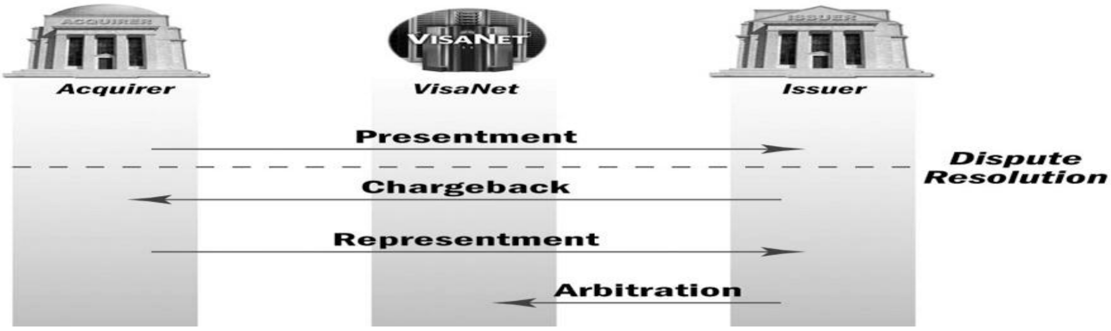


Figure -Courtesy: Visa international operating regulations.

The acquirer and its merchant may or may not accept the charge back. In case it is not accepted, there will be a representment case. In case the issuer is still not satisfied with the same, it can opt for arbitration. The primary responsibility of the charge-back payment lies with the acquirer irrespective of whether the loss it made good by the merchant; the charge back has to be honored by the issuer.

The charge back process and crediting the customer is totally decoupled. When a dispute has been raised by the card holder and the card holder's account has already been debited, the charge-back amount needs to be credited to the cardholder's account immediately, irrespective of whether the charge-back is initiated or no. The dispute on a transaction is subject to certain terms and conditions.

i. Charge-back process

Visa and Master have defined specific codes to identify various charge-backs. The internal guidelines of Master and Visa insist that all the charge-backs have to happen through specific software and not through mails, fax or any non-automated methods. All charge-backs and representments must be supported with enough documentary evidence and must be done within eight calendar days. Each transaction has to be charged back separately. The issuer cannot combine transactions and charge them back as a single transaction.

In case of the US, the following applies:

- The issuer should provide the cardholder's address, subject to the applicable law, if requested by the acquirer.
- An acquirer must not process a transaction as a first presentment if the transaction was previously charged back.

ii. Charge-back reason codes

Every charge-back has to be tagged a reason code for identification and analysis. The reason codes of Visa are as follows:

Reason Code	**Reason Description**
30	Services not provided or merchandise not received
41	Cancelled recurring transaction
53	Not as described or defective merchandise
57	Fraudulent multiple transactions
60	Illegible fulfillment
62	Counterfeit transaction
70	Card recovery bulletin or exception file
71	Declined authorization
72	No authorization
73	Expired card
74	Late presentment

75	Transaction not recognized
76	Incorrect currency or transaction code or domestic transaction processing violation
77	Non-matching account number
78	Service code violation
80	Incorrect transaction amount or account number
81	Fraud- card present environment
82	Duplicate processing
83	Fraud- card absent environment
85	Credit not processed
86	Paid by other means
90	Non-receipt of cash or load transaction value at ATM or load device
93	Merchant fraud performance program
96	Transaction exceeding limited amount

The time limit for the charge-back is calculated from the transaction processing date and begins from the calendar day following the transaction processing date.

The acquirer may represent to the issuer a charge back within 45 calendar days from the date of charge-back processing by the issuer. The reason for representment also needs to be communicated back to the issuer. There are representation codes defined for the same.

For each reason code for charge-back, there can be different timelines within which the charge-back must be submitted with minimum threshold limit above which the charge back can be requested. The documentation requirements are also elaborate for the charge-back process.

iii. Arbitration

Arbitration allows Visa to assign liability for a disputed Transaction when the charge-back and representment process fails to resolve the dispute. If an issuer disputes a Representment from an acquirer, the issuer may file for arbitration with Visa. In arbitration, Visa decides which party is responsible for the disputed transaction. The decision by Visa is final, except for any right of appeal permitted, and must be accepted by the issuer and acquirer. During arbitration, the Arbitration and Compliance Committee reviews all documentation/information submitted by both members to determine who has final liability for the transaction. The filing Member is liable for any difference due to currency fluctuation between the amount originally presented and the chargeback or representment amount.

iv. Chargeback Monitoring Program

Any charge back can lead to a reputation risk for all the participants in the card market. The chargeback is closely monitored by Visa/Master on an ongoing basis.

The charge-backs have to be monitored at:

- Acquirer level
- Merchant level
- Merchant outlet level

Visa monitors the total volume of US Domestic and International Interchange and charge-back for any US acquirers that have all of the following activities:

- 500 or more interchange transactions

- 500 or more charge-backs
- A 1.00% or higher ratio of overall charge-back to interchange volumes

Visa monitors the total volume of US Domestic and International Interchange and chargeback for single merchant outlets and identifies those with following activities:

- 100 or more interchange transactions
- 100 or more charge backs
- A 1.00% or higher ratio of overall charge-back to interchange volumes

An acquirer may submit interchange for a single merchant outlet under multiple names. Under such circumstances, Visa will group the merchant activity and notify the respective acquirer of the interchange grouping.

Visa also monitors the merchant outlets and can place a merchant outlet in the Global Merchant Chargeback monitoring program if any of its outlets meets or exceeds all the following monthly performance activity levels for international transactions:

- 200 charge backs
- 200 transactions
- 2.0% ratio of chargeback to transactions

Every chargeback is charged not less than $100. The major chunk will be passed on to the issuer while Visa will retain a part of the fees as administrative fees. The fees are in initial stages. There are stringent penalties both at the merchant and acquirer levels. The maximum penalty is revoking of the merchant/acquirer license.

10. Card Fees:

a. Introduction

All market participants are in the business for profit. Advertisements of these participants lure customers by offers such as life-time free cards, etc. The charges and fees of the card issuer are very confusing. To make the process and charges transparent, the regulator has taken a number of steps to enact a number of regulations.

The charges and fees can be broadly classified into transaction related fees such as interchange fees at the time of clearing and settlement and card holder related fees charged by the issuer.

b. Transaction related fees and charges for customers

Nature of Fee	Fee description	Paid by /to	Remarks
ATM Fees	Charges for using the ATM	Card Holder to issuer	Can vary from country to country
ATM Interchange Fees	Charges paid by for using the ATM when the issuer is different from acquirer	Issuer to acquirer	In case Bob has an ATM card of Citibank and he withdraws cash from Wells Fargo Bank, Citibank has to pay fees to Wells Fargo for this transaction. This may or may not be passed

			on to Bob depending on local rules and regulations.
Convenience Fee	Charged to customers generally for non-face to face transactions	Card holder to issuer	
Recovered Card handling fees	Paid when a card is swallowed by an ATM and is sent to the issuer	Issuer to acquirer	
Reward for recovered Card	An issuer can also declare monetary rewards for recovery of certain cards where frauds have been identified or otherwise. The limits of the same are defined by Visa.	Issuer to acquirer	This reward can again be passed on to the merchant by the acquirer.
Transaction on Receipt Retrieval Fee	For every retrieval request for a transaction, the issuer is charged. A retrieval fee is charged under the following circumstances. Acquirer did not properly supply requested Transaction Receipt. • Substitute Transaction Receipt does not include required data • Request resulted from an incorrect Merchant description or	Issuer to acquirer	

	a zero-filled or incorrect Transaction. Date in the Visa Net transmission For US Domestic Transactions, one of the following: • Requested copy was illegible • Acquirer did not properly supply required healthcare auto-substantiation transaction details • The Acquirer may collect a US $25 handling fee from the issuer if the original clearing record contained one of the following: - Airline/railway passenger itinerary data - A "1" in the Lodging/Car Rental No Show Indicator		
Interchange fees		Acquirer to issuer and vice versa	In case of purchases the acquirer will pay to issuer. In case of cash transactions the issuer will pay to the acquirer (e.g. ATM Interchange fees mentioned above).

			In case of credit or chargeback the chargeback flow will be reverse
Merchant discount fee or Merchant service	Negotiated fee between the merchant and acquirer. It may have a number of components.	Merchant to acquirer	
Annual Maintenance Fee	Charged on specific card types and can vary from issuer to issuer	Cardholder to issuer	Some issuers waive the same also in the form of life-time free cards
Late Payment Charges	In the event of default of the installment payment the same will be levied	Cardholder to issuer	
Interest Charges	Interest levied on the card holder for delayed payment as well as on monthly repayment.	Card holder to issuer	This is over and above late fees. This charges is to cover cost of funds
Cash Payment fee	In the event the bill amount is paid in cash, there can be additional fees for handling of cash	Card holder to issuer	

c. Interchange reimbursement fee (IRF)

Visa decides the IRF and publishes it to its members. In the earlier section, we had seen more than 78 transaction types for Visa. The interchange fees are related to transaction types and different transaction types can have different interchange fees.

The interchange fees can vary from 1% to 3%. The same is recovered at the time of clearing itself as in the example in the clearing and settlement section.

d. Interest Charges

In case of delayed payment, the card holders will be charged interest. The details of the interest charging and appropriation have already been discussed in the regulatory section.

11. Credit Card Receivables Management

a. Introduction

The last leg is the management of receivables from the card holder. In case of debit cards, the amount is debited to the checking account of the card holder. In case of credit cards the account of the card holder is debited. In the issuer books, there will be a running account for every primary card holder. In case of add-on cards, the transactions will be debited to the primary card holders' account.

b. Billing Cycle

The bills will have a billing cycle. Generally, the billing cycle is monthly. It need not necessarily be a calendar month. In case of an issuer with huge number of cards, the issuer can follow a staggered billing cycle; for example, for Card no 1 to 30,000, the billing cycle may be 1st of every month, card no 3,00,001 to 6,00,000 may be billed on 8th of every month.

The local regulations can also stipulate the minimum time period between the bill generation and bill due date. The bills can be dispatched through snail mail of email. In case of email the PCI DSS will become applicable.

c. Bill payment mode

The bill can be payment in a number of modes. The modes can be:

- Cash Check
- Electronic Fund Transfer / Visa Transfer

In the case of cash and cheque deposit, the issuer can appoint agents through whom it can collect the payments. In case of checks, the popular method is drop boxes where the card holder drops the cheque. Drop boxes are provided at ATMs, shopping malls, metro stations etc. In case of cheque deposits, the date of credit should happen before due date to avoid delayed payment charges. In an electronic fund transfer route, there are two ways it is handled. The first method is the standing instruction given by the customer to the card issuer to debit his checking account for the bill. This is a one-time instruction. In the second method, the card holder logs in on the Internet banking site and remits proceeds through the issuer. The exact methodology of the same can vary from geography to geography.

d. Delinquency Management

One of the biggest problems in the US due to the recession was huge spending by card holders on one side, and the inability to repay outstanding credit on the other. Over a period of time, the amount of outstanding mounted including interest. Accounts that are outstanding for more than a specified period will be classified as delinquent. The issuer has to approach the card holder to request him/her to repay. There are regulations in the manner in which the repayment can be requested as we seen in the regulations section. Delinquency can be handled in multiple ways such as rescheduling the payment period, giving interest rebates, and waiver of interest. Despite all these efforts, if it is not repaid, the issuer has no option but to write off the credit card debt, which will affect the bottom line of the issuer.

e. Loyalty Programs / Reward schemes

Every card holder has a loyalty program. The business rules for each loyalty program are defined by the issuer. The loyalty program is of different types. There can be partner loyalty programs such as partner airways, hotels etc. Standard software is available to handle complicated loyalty programs. The loyalty points can either be redeemed for gifts or even via payment of annual charges.

End of Document