

# Comparative analysis of private, public banks

Business



ibmr| study on impact of technology on customer needs in banking| | |

NAYANA SHREE N S| MBA FINANCE| Project on study on impact of technology on customer needs in banking SEMESTER IV SUBMITTED BY NAYANA SHREE

N S ROLL NO. IBMR COLLEGE IBMR COLLEGE Address: CERTIFICATE This is to certify that Nayana Shree N S of MBA FINANCE Semester IV {2012-13} has

successfully completed the project on “ Project on study on impact of technology on customer needs in banking” under the guidance of Mrs.

Bickram . Course Co-ordinatorPrincipal

Project Guide/ Internal Examiner External Examiner DECLARATION I Nayana Shree N S the student of MBA Finance Semester IV {2012-13} hereby declare that I have completed the project on “ Project on study on impact of technology on customer needs in banking”. The information submitted is true and original to the best of my knowledge.

Signature Nayana Shree N S Roll No. ACKNOWLEDGEMENT Many people have played a part in making this project study a success by giving their valuable inputs and useful suggestions.

Firstly I would express my gratitude to the University Of Mysore for providing me the opportunity to study the practical aspects of banking and insurance. I am thankful to the principal Mrs. xxxxxxx for giving me an opportunity to work on this project. I am also thankful to our co-ordinator Mrs.

xxxxxx for her immeasurable encouragement and support. I am also particularly grateful to my project guide xxxxx for extending his support and time. INDEX Chapter No. | Titles| Pg. No.

| 1| Introduction| 1-7| 2| Role Of Technology| 8| 3| E-Banking| 9-12| | Digital Signatures| 13-15| 5| Card Skimming| 16| 6| Credit Cards| 17-20| 7| Mobile Banking| 21-23| 8| Electronic Funds Transfer| 24-26| 9| Debit Cards| 27-33| 10| Telephone Banking| 34-35| 11| Uses Of Information Technology In Banks| 36-39| 12| Technology Vision 2020| 40-44| 13| Present Level of Computerization| 45-46| 14| Advantages of Technology| 47-48| 15| Disadvantages of Technology| 49-50| 16| Nature and Change in Banking| 51-53| 17| Issues and Challenges| 54| 18| Countermeasures to Frauds| 55-58| 19| Conclusion| 59| 20| Bibliography| 60| INTRODUCTION

In the five decades since independence, banking in India has evolved through four distinct phases. During Fourth phase, also called as Reform Phase, Recommendations of the Narasimham Committee (1991) paved the way for the reform phase in the banking. Important initiatives with regard to the reform of the banking system were taken in this phase. Important among these have been introduction of new accounting and prudential norms relating to income recognition, provisioning and capital adequacy, deregulation of interest rates & easing of norms for entry in the field of banking.

Entry of new banks resulted in a paradigm shift in the ways of banking in India.

The growing competition, growing expectations led to increased awareness amongst banks on the role and importance of technology in banking. The arrival of foreign and private banks with their superior state-of-the-art technology-based services pushed Indian Banks also to follow suit by going in for the latest technologies so as to meet the threat of competition and <https://assignbuster.com/comparative-analysis-of-private-public-banks/>

retain their customer base. Indian banking industry, today is in the midst of an IT revolution.

A combination of regulatory and competitive reasons have led to increasing importance of total banking automation in the Indian Banking Industry. Information Technology has basically been used under two different avenues in Banking. One is Communication and Connectivity and other is Business Process Reengineering.

Information technology enables sophisticated product development, better market infrastructure, implementation of reliable techniques for control of risks and helps the financial intermediaries to reach geographically distant and diversified markets.

In view of this, technology has changed the contours of three major functions performed by banks, i. e. , access to liquidity, transformation of assets and monitoring of risks. Further, Information technology and the communication networking systems have a crucial bearing on the efficiency of money, capital and foreign exchange markets. The Software Packages for Banking Applications in India had their beginnings in the middle of 80s, when the Banks started computerizing the branches in a limited manner.

The early 90s saw the plummeting hardware prices and advent of cheap and inexpensive but high-powered PCs and servers and banks went in for what was called Total Branch Automation (TBA) Packages. The middle and late 90s witnessed the tornado of financial reforms, deregulation, globalization etc. coupled with rapid revolution in communication technologies and evolution

of novel concept of 'convergence' of computer and communication technologies, like Internet, mobile / cell phones etc. MILESTONES

In India, banks as well as other financial entities entered the world of information technology and with Indian Financial Net (INFINET). INFINET, a wide area satellite based network (WAN) using VSAT (Very Small Aperture Terminals) technology, was jointly set up by the Reserve Bank and Institute for Development and Research in Banking Technology (IDRBT) in June 1999.

The Indian Financial Network (INFINET) which initially comprised only the public sector banks was opened up for participation by other categories of members.

The first set of applications that could benefit greatly from the use of technological advances in the computer and communications area relate to the Payment systems which form the lifeline of any banking activity. The process of reforms in payment and settlement systems has gained momentum with the implementation of projects such as NDS ((Negotiated Dealing System), CFMS (Centralised Funds Management System) for better funds management by banks and SFMS (Structured Financial Messaging Solution) for secure message transfer.

This would result in funds transfers and funds-related message transfer to be routed electronically across banks using the medium of the INFINET. Negotiated dealing system (NDS), which has become operational since February 2002 and RTGS (Real Time Gross Settlement system) scheduled towards the end of 2003 are other major developments in the area. Internet has significantly influenced delivery channels of the banks.

Internet has emerged as an important medium for delivery of banking products & services.

Detailed guidelines of RBI for Internet Banking has prepared the necessary ground for growth of Internet Banking in India. The Information Technology Act, 2000 has given legal recognition to creation, transmission and retention of an electronic (or magnetic) data to be treated as valid proof in a court of law, except in those areas, which continue to be governed by the provisions of the Negotiable Instruments Act, 1881.

As stated in RBI's Annual Monetary and Credit Policy 2002-2003: " To reap the full benefits of such electronic message transfers, it is necessary that banks bestow sufficient attention on the computerization and networking of the branches situated at commercially important centers on a time-bound basis. Intra-city and intra-bank networking would facilitate in addressing the " last mile" problem which would in turn result in quick and efficient funds transfers across the country". Implementation of Centralized Funds Management System

The centralized funds management system (CFMS) provides for a centralized viewing of balance positions of the account holders across different accounts maintained at various locations of RBI.

While the first phase of the system covering the centralized funds enquiry system (CFES) has been made available to the users, the second phase comprising the centralized funds transfer system (CFTS) would be made available by the middle of 2003. So far, 54 banks have implemented the system at their treasuries/funds management branches.

Certification and Digital Signatures The mid-term Review of October 2002 indicated the need for information security on the network and the use of public key infrastructure (PKI) by banks. The Controller of Certifying Authorities, Government of India, have approved the Institute for Development and Research in Banking Technology (IDRBT) as a Certification Authority (CA) for digital signatures. Consequently, the process of setting up of registration authorities (RA) under the CA has commenced at various banks.

In addition to the negotiated dealing system (NDS), the electronic clearing service (ECS) and electronic funds transfer (EFT) are also being enhanced in terms of security by means of implementation of PKI and digital signatures using the facilities offered by the CA. Committee on Payment Systems In order to examine the entire gamut of the process of reforms in payment and settlement systems which would be culminating with the real time gross settlement (RTGS) system, a Committee on Payment Systems (Chairman: Dr. R. H.

Patil) was set up in 2002. The Committee, after examining the various aspects relating to payment and settlement systems, submitted its report in September 2002 along with a draft Payment Systems Bill.

The draft Bill provides, inter alia, a legal basis for netting, apart from empowering RBI to have regulatory and oversight powers over payment and settlement systems of the country. The report of the Committee was put on the RBI website for wider dissemination. The draft Bill has been forwarded to the Government. Multi-application Smart Cards

Recognizing the need for technology based payment products and the growing importance of smart card based payment flows, a pilot project for multi-application smart cards in conjunction with a few banks and vendors, under the aegis of the Ministry of Communications and Information Technology, Government of India, has been initiated. The project is aimed at the formulation of standards for multi-application smart cards on the basis of inter-operable systems and technological components of the entire system.

#### Special Electronic Funds Transfer

As indicated in the mid-term Review of October 2002, national EFT (NEFT) is being introduced using the backbone of the structured financial messaging system (SFMS) of the IDRBT.

NEFT would provide for movement of electronic transfer of funds in a safe, secure and quick manner across branches of any bank to any other bank through a central gateway of each bank, with the inter-bank settlement being effected in the books of account of banks maintained at RBI. Since this scheme requires connectivity across a large number of branches at many cities, a special EFT (SEFT) was introduced in April 2003 covering about 3000 branches in 500 cities.

This has facilitated same day transfer of funds across accounts of constituents at all these branches. National Settlement System (NSS) The clearing and settlement activities are dispersed through 1, 047 clearing houses managed by RBI, the State Bank of India and its associates, public sector banks and other institutions. In order to facilitate banks to have better control over their funds, it is proposed to introduce national settlement system (NSS) in a phased manner.

<https://assignbuster.com/comparative-analysis-of-private-public-banks/>



Real Time Gross Settlement System (RTGS) As indicated in the mid-term Review of October 2002, development of the various software modules for the RTGS system is in progress.

The initial set of modules is expected to be delivered by June 2003 for members to conduct tests and familiarisation exercises. The live run of RTGS is scheduled towards the end of 2003. Reporting of Call/Notice Money Market Transactions on NDS Platform Negotiated dealing system (NDS), which has become operational since February 2002, enables on-line dealing and dissemination of trade information relating to instruments in money, government securities and foreign exchange markets. Membership in NDS is open to all institutions which are members of INFINET and are maintaining subsidiary general ledger (SGL) Account with RBI.

These include banks, financial institutions (FIs), primary dealers (PDs), insurance companies, mutual funds and any other institution as admitted by RBI.

At present, all deals in government securities, call/notice/term money, CDs and CP executed among NDS members have to be reported automatically through NDS, if the deal is done on NDS and within 15 minutes of concluding the deal, if done outside NDS. However, it has been observed that a very sizeable proportion of daily call/notice money market deals is not reported by members on NDS as stipulated.

With a view to improving transparency and strengthening efficiency in the market, it is proposed that: 1. From the fortnight beginning May 3, 2003, it would be mandatory for all NDS members to report all their call/notice

money market deals on NDS. Deals done outside NDS should be reported within 15 minutes on NDS, irrespective of the size of the deal or whether the counterparty is a member of the NDS or not. 2.

Full compliance with the reporting requirement to NDS will be reviewed in September 2003.

In case there is repeated non-reporting of deals by an NDS member, it will be considered whether non-reported deals by that member should be treated as invalid with effect from a future date. ROLE OF TECHNOLOGY Information Technology has basically been used under two different avenues in Banking. One is Communication and Connectivity and other is Business Process Reengineering. Information technology enables sophisticated product development, better market infrastructure, implementation of reliable techniques for control of risks and helps the financial intermediaries to reach geographically distant and diversified markets.

In view of this, technology has changed the contours of three major functions performed by banks, i. e. , access to liquidity, transformation of assets and monitoring of risks. Further, Information technology and the communication networking systems have a crucial bearing on the efficiency of money, capital and foreign exchange markets. Internet has significantly influenced delivery channels of the banks.

Internet has emerged as an important medium for delivery of banking products ; services. Detailed guidelines of RBI for Internet Banking has prepared the necessary ground for growth of Internet Banking in India.

The Information Technology Act, 2000 has given legal recognition to creation, transmission and retention of an electronic (or magnetic) data to be treated as valid proof in a court of law, except in those areas, which continue to be governed by the provisions of the Negotiable Instruments Act, 1881. As stated in RBI's Annual Monetary and Credit Policy 2002-2003: " To reap the full benefits of such electronic message transfers, it is necessary that banks bestow sufficient attention on the computerisation and networking of the branches situated at commercially important centres on a time-bound basis.

Intra-city and intra-bank networking would facilitate in addressing the " last mile" problem which would in turn result in quick and efficient funds transfers across the country". E-BANKING Online banking (or Internet banking) allows customers to conduct financial transactions on a secure website operated by their retail or virtual bank, credit union or building society.

Online banking solutions have many features and capabilities in common, but traditionally also have some that are application specific. The common features fall broadly into several categories Transactional (e. g. , performing a financial transaction such as an account to account transfer, paying a bill, wire transfer, apply for a loan, new account, etc. ) \* Payments to third parties, including bill payments and telegraphic/wire transfers \* Funds transfers between a customer's own transactional account and savings accounts \* Investment purchase or sale \* Loan applications and transactions, such as repayments of enrollments \* Non-transactional (e.

g. , online statements, cheque links, cobrowsing, chat) \* Viewing recent transactions Downloading bank statements , for example in PDF format \* <https://assignbuster.com/comparative-analysis-of-private-public-banks/>

Viewing images of paid cheques \* Financial Institution Administration \*

Management of multiple users having varying levels of authority \*

Transaction approval process Features commonly unique to Internet banking include Personal financial management support, such as importing data into personal accounting software Some online banking platforms support account aggregation to allow the customers to monitor all of their accounts in one place whether they are with their main bank or with other institutions.

### History of E-Banking

The precursor for the modern home online banking services were the distance banking services over electronic media from the early 1980s. The term online became popular in the late '80s and referred to the use of a terminal, keyboard and TV (or monitor) to access the banking system using a phone line. ' Home banking' can also refer to the use of a numeric keypad to send tones down a phone line with instructions to the bank. Online services started in New York in 1981 when four of the city's major banks (Citibank, Chase Manhattan, Chemical andManufacturers Hanover) offered home banking services[1] using the videotex system.

Because of the commercial failure of videotex these banking services never became popular except in France where the use of videotex (Minitel) was subsidised by the telecom provider and the UK, where the Prestel system was used. The UK's first home online banking services[2] was set up by Bank of Scotland for customers of the Nottingham Building Society (NBS) in 1983. [3] The system used was based on the UK's Prestel system and used a computer, such as the BBC Micro, or keyboard (Tandata Td1400) connected to the telephone system and television set.

<https://assignbuster.com/comparative-analysis-of-private-public-banks/>

The system (known as 'Homelink') allowed on-line viewing of statements, bank transfers and bill payments. In order to make bank transfers and bill payments, a written instruction giving details of the intended recipient had to be sent to the NBS who set the details up on the Homelink system. Typical recipients were gas, electricity and telephone companies and accounts with other banks.

Details of payments to be made were input into the NBS system by the account holder via Prestel.

A cheque was then sent by NBS to the payee and an advice giving details of the payment was sent to the account holder. BACS was later used to transfer the payment directly. Stanford Federal Credit Union was the first financial institution to offer online internet banking services to all of its members in October 1994. [citation needed] Today, many banks are internet only banks. Unlike their predecessors, these internet only banks do not maintain brick and mortar bank branches.

Instead, they typically differentiate themselves by offering better interest rates and online banking features.

Security Protection through single password authentication, as is the case in most secure Internet shopping sites, is not considered secure enough for personal online banking applications in some countries. Basically there exist two different security methods for online banking. 1. The PIN/TAN system where the PIN represents a password, used for the login and TANs representing one-time passwords to authenticate transactions.

TANs can be distributed in different ways, the most popular one is to send a list of TANs to the online banking user by postal letter.

The most secure way of using TANs is to generate them by need using a security token. These token generated TANs depend on the time and a unique secret, stored in the security token (this is called two-factor authentication or 2FA). Usually online banking with PIN/TAN is done via a web browser using SSL secured connections, so that there is no additional encryption needed. Another way to provide TANs to an online banking user is to send the TAN of the current bank transaction to the user's (GSM) mobile phone via SMS. The SMS text usually quotes the transaction amount and details, the TAN is only valid for a short period of time.

Especially in Germany and Austria, many banks have adopted this "SMS TAN" service as it is considered very secure. 2. Signature based online banking where all transactions are signed and encrypted digitally. The Keys for the signature generation and encryption can be stored on smartcards or any memory medium, depending on the concrete implementation. Attacks Most of the attacks on online banking used today are based on deceiving the user to steal login data and valid TANs. Two well known examples for those attacks are phishing and pharming.

Cross-site scripting and keylogger/Trojan horses can also be used to steal login information.

A method to attack signature based online banking methods is to manipulate the used software in a way, that correct transactions are shown on the screen and faked transactions are signed in the background. A recent FDIC

Technology Incident Report, compiled from suspicious activity reports banks file quarterly, lists 536 cases of computer intrusion, with an average loss per incident of \$30, 000. That adds up to a nearly \$16-million loss in the second quarter of 2007. Computer intrusions increased by 150 percent between the first quarter of 2007 and the second.

In 80 percent of the cases, the source of the intrusion is unknown but it occurred during online banking, the report states.

The most recent kind of attack is the so-called Man in the Browser attack, where a Trojan horse permits a remote attacker to modify the destination account number and also the amount. Countermeasures There exist several countermeasures which try to avoid attacks. Digital certificates are used against phishing and pharming, the use of class-3 card readers is a measure to avoid manipulation of transactions by the software in signature based online banking variants.

To protect their systems against Trojan horses, users should use virus scanners and be careful with downloaded software or e-mail attachments.

**DIGITAL SIGNATURES** A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit.

Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. In some countries, including the United States, India, and members of the European Union, electronic signatures have legal significance. However, laws concerning electronic signatures do not always make clear whether they are digital cryptographic signatures in the sense used here, leaving the legal definition, and so their importance, somewhat confused.

Digital signatures employ a type of asymmetric cryptography.

For messages sent through a nonsecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective.

Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless. Digitally signed messages may be anything representable as a bitstring: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol. A digital signature scheme typically consists of three algorithms: 1.



A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. 2. A signing algorithm that, given a message and a private key, produces a signature. 3.

A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key.

Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key. Uses of digital signatures As organizations move away from paper documents with ink signatures or authenticity stamps, digital signatures can provide added assurances of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory. The United States Government Printing Office (GPO) publishes electronic versions of the budget, public and private laws, and congressional bills with digital signatures.

Universities including Penn State, University of Chicago, and Stanford are publishing electronic student transcripts with digital signatures. Below are some common reasons for applying a digital signature to communications: Authentication Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When

ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user.

The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account.

If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

**Integrity** In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission.

Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not. ) However, if a message is digitally signed, any change in the message after signature will invalidate the signature.

Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance). Digital signatures vs. ink on paper signatures An ink signature can be easily replicated from one document to another by copying the image manually or digitally. Digital signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document. Paper contracts

often have the ink signature block on the last page, and the previous pages may be replaced after a signature is applied. Digital signatures can be applied to an entire document, such that the digital signature on the last page will indicate tampering if any data on any of the pages have been altered.

**CARD SKIMMING** Card skimming' is the illegal copying of information from the magnetic strip of a credit or ATM card. It is a more direct version of a phishing scam. The scammers try to steal your details so they can access your accounts. Once scammers have skimmed your card, they can create a fake or 'cloned' card with your details on it. The scammer is then able to run up charges on your account.

Card skimming is also a way for scammers to steal your identity (your personal details) and use it to commit identity fraud. By stealing your personal details and account numbers the scammer may be able to borrow money or take out loans in your name.

Warning signs

- A shop assistant takes your card out of your sight in order to process your transaction.
- You are asked to swipe your card through more than one machine.
- You see a shop assistant swipe the card through a different machine to the one you used.
- You notice something suspicious about the card slot on an ATM (e.

g. an attached device).

- You notice unusual or unauthorised transactions on your account or credit card statement. Protect yourself from card skimming

- Keep your credit card and ATM cards safe. Do not share your personal

identity number (PIN) with anyone. Do not keep any written copy of your PIN with the card.

Check your bank account and credit card statements when you get them. If you see a transaction you cannot explain, report it to your credit union or bank. •Choose passwords that would be difficult for anyone else to guess.

**CREDIT CARDS** A credit card is a small plastic card issued to users as a system of payment. It allows its holder to buy goods and services based on the holder's promise to pay for these goods and services.

[1] The issuer of the card creates a revolving account and grants a line of credit to the consumer (or the user) from which the user can borrow money for payment to a merchant or as a cash advance to the user.

A credit card is different from a charge card: a charge card requires the balance to be paid in full each month. In contrast, credit cards allow the consumers a continuing balance of debt, subject to interest being charged. A credit card also differs from a cash card, which can be used like currency by the owner of the card. Most credit cards are issued by banks or credit unions, and are the shape and size specified by the ISO/IEC 7810 standard as ID-1. This is defined as 85.

60 ? 53. 98 mm (3. 370 ? 2. 125 in) (33/8 ? 21/8 in) in size .

**How credit cards work** Credit cards are issued by a credit card issuer, such as a bank or credit union, after an account has been approved by the credit provider, after which cardholders can use it to make purchases at merchants accepting that card. Merchants often advertise which cards they accept by

displaying acceptance marks - generally derived from logos - or may communicate this orally, as in "Credit cards are fine" (implicitly meaning "major brands"), "We take (brands X, Y, and Z)", or "We don't take credit cards".

When a purchase is made, the credit card user agrees to pay the card issuer. The cardholder indicates consent to pay by signing a receipt with a record of the card details and indicating the amount to be paid or by entering a personal identification number (PIN). Also, many merchants now accept verbal authorizations via telephone and electronic authorization using the Internet, known as a card not present transaction (CNP).

Electronic verification systems allow merchants to verify in a few seconds that the card is valid and the credit card customer has sufficient credit to cover the purchase, allowing the verification to happen at time of purchase. The verification is performed using a credit card payment terminal or point-of-sale (POS) system with a communications link to the merchant's acquiring bank. Data from the card is obtained from a magnetic stripe or chip on the card; the latter system is called Chip and PIN in the United Kingdom and Ireland, and is implemented as an EMV card.

For card not present transactions where the card is not shown (e. g. , e-commerce, mail order, and telephone sales), merchants additionally verify that the customer is in physical possession of the card and is the authorized user by asking for additional information such as the security code printed on the back of the card, date of expiry, and billing address. Each month, the credit card user is sent a statement indicating the purchases undertaken with the card, any outstanding fees, and the total amount owed.

After receiving the statement, the cardholder may dispute any charges that he or she thinks are incorrect (see 15 U.

S. C. § 1643, which limits cardholder liability for unauthorized use of a credit card to \$50, and the Fair Credit Billing Act for details of the US regulations). Otherwise, the cardholder must pay a defined minimum proportion of the bill by a due date, or may choose to pay a higher amount up to the entire amount owed. The credit issuer charges interest on the amount owed if the balance is not paid in full (typically at a much higher rate than most other forms of debt).

In addition, if the credit card user fails to make at least the minimum payment by the due date, the issuer may impose a “late fee” and/or other penalties on the user.

To help mitigate this, some financial institutions can arrange for automatic payments to be deducted from the user’s bank accounts, thus avoiding such penalties altogether as long as the cardholder has sufficient funds. Interest charges Credit card issuers usually waive interest charges if the balance is paid in full each month, but typically will charge full interest on the entire outstanding balance from the date of each purchase if the total balance is not paid.

For example, if a user had a \$1, 000 transaction and repaid it in full within this grace period, there would be no interest charged. If, however, even \$1. 00 of the total amount remained unpaid, interest would be charged on the \$1, 000 from the date of purchase until the payment is received. The precise

manner in which interest is charged is usually detailed in a cardholder agreement which may be summarized on the back of the monthly statement.

The general calculation formula most financial institutions use to determine the amount of interest to be charged is  $APR/100 \times ADB/365 \times \text{number of days revolved}$ .

Take the annual percentage rate (APR) and divide by 100 then multiply to the amount of the average daily balance (ADB) divided by 365 and then take this total and multiply by the total number of days the amount revolved before payment was made on the account. Financial institutions refer to interest charged back to the original time of the transaction and up to the time a payment was made, if not in full, as RRFC or residual retail finance charge.

Thus after an amount has revolved and a payment has been made, the user of the card will still receive interest charges on their statement after paying the next statement in full (in fact the statement may only have a charge for interest that collected up until the date the full balance was paid, i. e.

when the balance stopped revolving). The credit card may simply serve as a form of revolving credit, or it may become a complicated financial instrument with multiple balance segments each at a different interest rate, possibly with a single umbrella credit limit, or with separate credit limits applicable to the various balance segments.

Usually this compartmentalization is the result of special incentive offers from the issuing bank, to encourage balance transfers from cards of other issuers. In the event that several interest rates apply to various balance

segments, payment allocation is generally at the discretion of the issuing bank, and payments will therefore usually be allocated towards the lowest rate balances until paid in full before any money is paid towards higher rate balances.

Interest rates can vary considerably from card to card, and the interest rate on a particular card may jump dramatically if the card user is late with a payment on that card or any other credit instrument, or even if the issuing bank decides to raise its revenue.

**Benefits to customers** The main benefit to each customer is convenience.

Compared to debit cards and cheques, a credit card allows small short-term loans to be quickly made to a customer who need not calculate a balance remaining before every transaction, provided the total charges do not exceed the maximum credit line for the card.

Credit cards also provide more fraud protection than debit cards. In the UK for example, the bank is jointly liable with the merchant for purchases of defective products over ? 100. [5] Many credit cards offer rewards and benefits packages, such as offering enhanced product warranties at no cost, free loss/damage coverage on new purchases, and points which may be redeemed for cash, products, or airline tickets. Additionally, carrying a credit card may be a convenience to some customers as it eliminates the need to carry any cash for most purposes.

**MOBILE BANKING** Mobile banking (also known as M-Banking, mbanking, SMS Banking) is a term used for performing balance checks, account transactions, payments, credit applications and other banking transactions through a



mobile device such as a mobile phone or Personal Digital Assistant (PDA). The earliest mobile banking services were offered over SMS. With the introduction of the first primitive smart phones with WAP support enabling the use of the mobile web in 1999, the first European banks started to offer mobile banking on this platform to their customers .

Mobile banking has until recently (2010) most often been performed via SMS or the Mobile Web. Apple's initial success with iPhone and the rapid growth of phones based on Google's Android (operating system) have led to increasing use of special client programs, called apps, downloaded to the mobile device. Mobile Banking Services Mobile banking can offer services such as the following: Account Information 1. Mini-statements and checking of account history 2. Alerts on account activity or passing of set thresholds 3. Monitoring of term deposits 4. Access to loan statements 5. Access to card statements . Mutual funds / equity statements 7. Insurance policy management 8. Pension plan management 9.

Status on cheque, stop payment on cheque 10. Ordering cheque books 11. Balance checking in the account 12. Recent transactions 13. Due date of payment (functionality for stop, change and deleting of payments) 14. PIN provision, Change of PIN and reminder over the Internet 15.

Blocking of (lost, stolen) cards Payments, Deposits, Withdrawals, and Transfers 1. Domestic and international fund transfers 2. Micro-payment handling 3. Mobile recharging 4. Commercial payment processing 5.

Bill payment processing . Peer to Peer payments 7. Withdrawal at banking agent 8. Deposit at banking agent A specific sequence of SMS messages will <https://assignbuster.com/comparative-analysis-of-private-public-banks/>

enable the system to verify if the client has sufficient funds in his or her wallet and authorize a deposit or withdrawal transaction at the agent. When depositing money, the merchant receives cash and the system credits the client's bank account or mobile wallet.

In the same way the client can also withdraw money at the merchant: through exchanging sms to provide authorization, the merchant hands the client cash and debits the merchant's account. Investments 1.

Portfolio management services 2. Real-time stock quotes 3. Personalized alerts and notifications on security prices Support 1.

Status of requests for credit, including mortgage approval, and insurance coverage 2. Check (cheque) book and card requests 3. Exchange of data messages and email, including complaint submission and tracking 4. ATM Location Content Services 1. General information such as weather updates, news 2. Loyalty-related offers 3.

Location-based services Based on a survey conducted by Forrester, mobile banking will be attractive mainly to the younger, more "tech-savvy" customer segment.

A third of mobile phone users say that they may consider performing some kind of financial transaction through their mobile phone. But most of the users are interested in performing basic transactions such as querying for account balance and making bill payment. ELECTRONIC FUNDS TRANSFER Electronic funds transfer or EFT is the electronic exchange or transfer of money from one account to another, either within a single financial

institution or across multiple institutions, through computer-based systems. The term is used for a number of different concepts: Cardholder-initiated transactions, where a cardholder makes use of a payment card \* Direct deposit payroll payments for a business to its employees, possibly via a payroll service bureau \* Direct debit payments, sometimes called electronic checks, for which a business debits the consumer's bank accounts for payment for goods or services \* Electronic bill payment in online banking, which may be delivered by EFT or paper check \* Transactions involving stored value of electronic money, possibly in a private currency \* Wire transfer via an international banking network (carries a higher fee in North America) \* Electronic Benefit Transfer In 1978 U. S.

Congress passed the Electronic Funds Transfer Act to establish the rights and liabilities of consumers as well as the responsibilities of all participants in EFT activities in the United States. RTGS

Real time gross settlement systems (RTGS) are funds transfer systems where transfer of money or securities[1] takes place from one bank to another on a " real time" and on " gross" basis. Settlement in " real time" means payment transaction is not subjected to any waiting period. The transactions are settled as soon as they are processed. " Gross settlement" means the transaction is settled on one to one basis without bunching or netting with any other transaction. Once processed, payments are final and irrevocable.

Fees for RTGS vary from bank to bank. RBI has prescribed upper limit for the fees which can be charged by all banks both for NEFT and RTGS.

Both the remitting and receiving must have Core banking in place to enter into RTGS transactions. Core Banking enabled banks and branches are assigned an Indian Financial System Code (IFSC) for RTGS and NEFT purposes. This is an eleven digit alphanumeric code and unique to each branch of bank.

The first four alphabets indicate the identity of the bank and remaining seven numerals indicate a single branch. This code is provided on the cheque books, which are required for transactions along with recipient's account number. RTGS is a large value (minimum value of transaction should be Rs 2, 00, 000) funds transfer system whereby financial intermediaries can settle interbank transfers for their own account as well as for their customers.

The system effects final settlement of interbank funds transfers on a continuous, transaction-by-transaction basis throughout the processing day. Customers can access the RTGS facility between 9 am to 4: 30 pm on week days and 9 am to 1: 30 pm on Saturday.

However, the timings that the banks follow may vary depending on the customer timings of the bank branches. Banks could use balances maintained under the cash reserve ratio (CRR) and the intra-day liquidity (IDL) to be supplied by the central bank, for meeting any eventuality arising out of the real time gross settlement (RTGS). The RBI fixed the IDL limit for banks to three times their net owned fund (NOF). The IDL will be charged at Rs 25 per transaction entered into by the bank on the

RTGS platform. The marketable securities and treasury bills will have to be placed as collateral with a margin of five per cent. However, the apex bank will also impose severe penalties if the IDL is not paid back at the end of the day.

National Electronic Fund Transfer National Electronic Fund Transfer (NEFT) is an online system for transferring funds of Indian financial institution (especially banks). There is no minimum limit for fund transfer in NEFT system. DEBIT CARDS A debit card (also known as a bank card or check card) is a plastic card that provides the cardholder electronic access to his or her bank account/s at a financial institution.

Some cards have a stored value with which a payment is made, while most relay a message to the cardholder's bank to withdraw funds from a designated account in favor of the payee's designated bank account. The card can be used as an alternative payment method to cash when making purchases.

In some cases, the cards are designed exclusively for use on the Internet, and so there is no physical card. In many countries the use of debit cards has become so widespread that their volume of use has overtaken or entirely replaced the check and, in some instances, cash transactions. Like credit cards, debit cards are used widely for telephone and Internet purchases. However, unlike credit cards, the funds paid using a debit card are transferred immediately from the bearer's bank account, instead of having the bearer pay back the money at a later date.

Debit cards usually also allow for instant withdrawal of cash, acting as the ATM card for withdrawing cash and as a check guarantee card. Merchants may also offer cashback facilities to customers, where a customer can withdraw cash along with their purchase.

**Online Debit System** Online debit cards require electronic authorization of every transaction and the debits are reflected in the user's account immediately. The transaction may be additionally secured with the personal identification number (PIN) authentication system and some online cards require such authentication for every transaction, essentially becoming enhanced automatic teller machine(ATM) cards.

One difficulty in using online debit cards is the necessity of an electronic authorization device at the point of sale (POS) and sometimes also a separate PINpad to enter the PIN, although this is becoming commonplace for all card transactions in many countries. Overall, the online debit card is generally viewed as superior to the offline debit card because of its more secure authentication system and live status, which alleviates problems with processing lag on transactions that may only issue online debit cards. Some on-line debit systems are using the normal authentication processes of Internet banking to provide real-time on-line debit transactions.

The most notable of these are Ideal and POLi. **Offline Debit System**

Offline debit cards have the logos of major credit cards (for example, Visa or MasterCard) or major debit cards (for example, Maestro in the United Kingdom and other countries, but not the United States) and are used at the point of sale like a credit card (with payer's signature). This type of debit

card may be subject to a daily limit, and/or a maximum limit equal to the current/checking account balance from which it draws funds. Transactions conducted with offline debit cards require 2-3 days to be reflected on users' account balances. In some countries and with some banks and merchant service organizations, a "credit" or offline debit transaction is without cost to the purchaser beyond the face value of the transaction, while a small fee may be charged for a "debit" or online debit transaction (although it is often absorbed by the retailer).

Other differences are that online debit purchasers may opt to withdraw cash in addition to the amount of the debit purchase (if the merchant supports that functionality); also, from the merchant's standpoint, the merchant pays lower fees on online debit transaction as compared to "credit" (offline) debit transaction. Prepaid debit cards Prepaid debit cards, also called reloadable debit cards or reloadable prepaid cards, are often used for recurring payments. The payer loads funds to the cardholder's card account. Prepaid debit cards use either the offline debit system or the online debit system to access these funds. Particularly for companies with a large number of payment recipients abroad, prepaid debit cards allow the delivery of international payments without the delays and fees associated with international checks and bank transfers.

Providers include Caxton FX prepaid cards, Escape prepaid cards, Travelex prepaid cards and TransCash prepaid Visa cards. Whereas, web-based services such as stock photography websites (istockphoto), outsourced services (oDesk), money transfer services (Western Union) and affiliate networks (MediaWhiz) have all started offering prepaid debit cards for their

contributors/freelancers/vendors. Advantages of debit cards a. A consumer who is not credit worthy and may find it difficult or impossible to obtain a credit card can more easily obtain a debit card, allowing him/her to make plastic transactions. For example, legislation often prevents minors from taking out debt, which includes the use of a credit card, but not online debit card transactions. b.

For most transactions, a check card can be used to avoid check writing altogether. Check cards debit funds from the user's account on the spot, thereby finalizing the transaction at the time of purchase, and bypassing the requirement to pay a credit card bill at a later date, or to write an insecure check containing the account holder's personal information. c. Like credit cards, debit cards are accepted by merchants with less identification and scrutiny than personal checks, thereby making transactions quicker and less intrusive. Unlike personal checks, merchants generally do not believe that a payment via a debit card may be later dishonored. d.

Unlike a credit card, which charges higher fees and interest rates when a cash advance is obtained, a debit card may be used to obtain cash from an ATM or a PIN-based transaction at no extra charge, other than a foreign ATM fee. Disadvantages of debit cards a. Use of a debit card is not usually limited to the existing funds in the account to which it is linked, most banks allow a certain threshold over the available bank balance which can cause overdraft fees if the users transaction does not reflect available balance. b. Many banks are now charging over-limit fees or non-sufficient funds fees based upon pre-authorizations, and even attempted but refused transactions by the



merchant (some of which may be unknown until later discovery by account holder).

c. Many merchants mistakenly believe that amounts owed can be “ taken” from a customer’s account after a debit card (or number) has been presented, without agreement as to date, payee name, amount and currency, thus causing penalty fees for overdrafts, over-the-limit, amounts not available causing further rejections or overdrafts, and rejected transactions by some banks. d. In some countries debit cards offer lower levels of security protection than credit cards. [9] Theft of the users PIN using skimming devices can be accomplished much easier with a PIN input than with a signature-based credit transaction.

However, theft of users’ PIN codes using skimming devices can be equally easily accomplished with a debit transaction PIN input, as with a credit transaction PIN input, and theft using a signature-based credit transaction is equally easy as theft using a signature-based debit transaction.

e. In many places, laws protect the consumer from fraud much less than with a credit card. While the holder of a credit card is legally responsible for only a minimal amount of a fraudulent transaction made with a credit card, which is often waived by the bank, the consumer may be held liable for hundreds of dollars, or even the entire value of fraudulent debit transactions. The consumer also has a shorter time (usually just two days) to report such fraud to the bank in order to be eligible for such a waiver with a debit card,[9] whereas with a credit card, this time may be up to 60 days.

A thief who obtains or clones a debit card along with its PIN may be able to clean out the consumer's bank account, and the consumer will have no recourse.

f. An automated teller machine (ATM), also known as a Cash Point, Cash Machine or sometimes a Hole in the Wall in British English, is a computerised telecommunications device that provides the clients of a financial institution with access to financial transactions in a public space without the need for a cashier, human clerk or bank teller. ATMs are known by various other names including automatic banking machine, cash machine, and various regional variants derived from trademarks on ATM systems held by particular banks.

g.

On most modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smart card with a chip, that contains a unique card number and some security information such as an expiration date or CVVC (CVV). Authentication is provided by the customer entering a personal identification number (PIN).

h. Using an ATM, customers can access their bank accounts in order to make cash withdrawals, credit card cash advances, and check their account balances as well as purchase prepaid cellphone credit. If the currency being withdrawn from the ATM is different from that which the bank account is denominated in (e. g. Withdrawing Japanese Yen from a bank account containing US Dollars), the money will be converted at a wholesale exchange rate. Thus, ATMs often provide the best possible exchange rate for foreign travelers and are heavily used for this purpose as well Alternative uses Two NCR Personas 84 ATMs at a bank in Jersey dispensing two types of pound <https://assignbuster.com/comparative-analysis-of-private-public-banks/>

sterling banknotes: Bank of England notes on the left, and States of Jersey notes on the right. Although ATMs were originally developed as just cash dispensers, they have evolved to include many other bank-related functions.

In some countries, especially those which benefit from a fully integrated cross-bank ATM network (e. g. Multibanco in Portugal), ATMs include many functions which are not directly related to the management of one's own bank account, such as:

1. Deposit currency recognition, acceptance, and recycling [61][62]
2. Paying routine bills, fees, and taxes (utilities, phone bills, social security, legal fees, taxes, etc.

3. Printing bank statements
4. Updating passbooks
5. Loading monetary value into stored value cards
6. Purchasing
- 7.

8. Lottery tickets
9. Train tickets
10. Concert tickets
11. Movie tickets
- 12.

13. Games and promotional features
14. Shopping mall gift certificates
15. Fast loans
16. CRM at the ATM

17. Adding pre-paid cell phone / mobile phone credit.

Increasingly banks are seeking to use the ATM as a sales device to deliver pre approved loans and targeted advertising using products such as ITM (the Intelligent Teller Machine) from Apra Relate from NCR. ATMs can also act as an advertising channel for companies to advertise their own products or third-party products and services. In Canada, ATMs are called guichets automatiques in French and sometimes " Bank Machines" in English. The <https://assignbuster.com/comparative-analysis-of-private-public-banks/>

Interac shared cash network does not allow for the selling of goods from ATMs due to specific security requirements for PIN entry when buying goods.

CIBC machines in Canada, are able to top-up the minutes on certain pay as you go phones. TELEPHONE BANKING

Telephone banking is a service provided by a financial institution, which allows its customers to perform transactions over the telephone. Most telephone banking services use an automated phone answering system with phone keypad response or voice recognition capability. To guarantee security, the customer must first authenticate through a numeric or verbal password or through security questions asked by a live representative (see below). With the obvious exception of cash withdrawals and deposits, it offers virtually all the features of an automated teller machine: account balance information and list of latest transactions, electronic bill payments, funds transfers between a customer's accounts, etc.

Usually, customers can also speak to a live representative located in a call centre or a branch, although this feature is not always guaranteed to be offered 24/7.

In addition to the self-service transactions listed earlier, telephone banking representatives are usually trained to do what was traditionally available only at the branch: loan applications, investment purchases and redemptions, chequebook orders, debit card replacements, change of address, etc. Banks which operate mostly or exclusively by telephone are known as phone banks. They also help modernise the user by using special technology. A credit card balance transfer is the transfer of the balance (the

money) in a credit card account to an account held at another credit card company.

This process is actively encouraged by almost all credit card issuers as a means to attract new customers.

Such an arrangement is attractive to the consumer because the new bank or credit card issuer will offer incentives such as a low interest or interest-free period, loyalty points or some such other device or combination of incentives. It is also attractive to the credit card company which uses this process to gain that new customer, and of course detrimental to the prior credit card company. An order of payments for every credit card specifies which balance(s) will be paid first. In nearly all cases payments apply to lowest-rate balances first - highest-rate last.

Any balance under a teaser rate or fixed rate will be paid off sooner than any purchases or cash advances (which usually have the highest APR).

By avoiding making purchases or taking cash advances altogether, the borrower can ensure they maintain the full benefits of the original balance transfer. The process is extremely fast and can be concluded within a matter of hours in some cases. Automated services exist to help facilitate such balance transfers. Other similar services do exist, but they may not be free to use. USES OF INFORMATION TECHNOLOGY IN BANKS Information

Technology uses in Banking sector: - •Business banking •Retail banking  
•Banking technology •Banking environment •Card Market Business banking:

BMI-Tec Knowledge has been publishing their annual report on Business Electronic Banking for the past 13 years.

<https://assignbuster.com/comparative-analysis-of-private-public-banks/>

The report provides valuable year on year trend analysis for the major banks in South Africa. There are two parallel research objectives of the publication, to report on business banking trends and more specific information on each of the electronic banking products offered by the banks. Each year, the questionnaire used for the research process retains a generic core but incorporates changes that reflect the ever changing banking environment and the related impact of technology. The research is focused on business banking and specifically for companies that use an online or electronic banking product in their day-to-day administration of their business banking administration. The key area of segmentation for this report is by the four major banks in South Africa: Absa, First National Bank, Nedbank and Standard Bank. Other areas of segmentation include size of company by employees and annual turnover and whether these companies are single banked or multi banked.

Retail banking: Understanding the financial delivery channels BMI-T has conducted a recent benchmarking study to highlight external expertise and knowledge that is currently available in the ATM and SST environment. From this collated information, the client was able will be able to benchmark their own operations against these parameters.

This study assisted the client in identifying and determining the current and potential best practices around ATMs and to see where they are currently placed in this context. The scope of the research covered both local and international perspectives with the international perspective be segmented further by a split between Africa in comparison with the Rest of the World and South Africa Business Electronic Banking in the Small to Medium

<https://assignbuster.com/comparative-analysis-of-private-public-banks/>

Business sector BMI-Tec Knowledge has been publishing their annual report on Business Electronic Banking in the corporate sector for the past 13 years. This new report, Business electronic banking in the SMB sector will be a parallel report in order to fully understand both markets; corporates and the SMB sector.

There are two parallel research objectives of the publication, to report on business banking trends in the small to medium business sector and provide more specific information on each of the electronic banking products offered by the banks.

The research is focused on business banking and specifically for companies that use an online or electronic banking product in their day-to-day administration of their business banking administration. The key area of segmentation for this report is the four major banks in South Africa: Absa, First National Bank, Nedbank and Standard Bank. Other areas of segmentation include size of company by employees and annual turnover and whether these companies are single banked or multi banked. Multi-Channel Banking for Retail Financial Services 2005: BMI-T conducts research in the financial delivery channels to the retail market.

This research covers the following issues: •The optimum balance between customer experience and lower costs, •International overview of financial delivery channels and the road to multi-channel integration, •Trends and market drivers and/or inhibitors that have driven the changes in global banks, •South African comparison of financial delivery channels and their related offerings from the banks, •Comparison of pricing and products and services that are available on each channel from each financial provider, <https://assignbuster.com/comparative-analysis-of-private-public-banks/>

- Number of customer points such as ATMs,
- Number of banking branches and level of change and expected growth for the future. Research to test the future for High-value-low frequency channels or low-value-high frequency channels, current and future usage patterns of financial delivery channels from the South African retail customers (which channels, frequency, timing and for which transactions plus trend analysis with past annual data).

Banking technology: South Africa is in many ways a global leader in the adoption and use of technology to improve competitiveness and de