Naavi

Na.Vijayashankar
"Ujvala", 37/5, 20th Main, B.S.K. Stage I, Bangalore 560050
Ph:/Fax:26603490: E-Mail: naavi@vsnl.com
Web: www.naavi.org

Damodaran Committee Recommendation (August 3 2011)	**Guidelines of 28th February 2013**
Internet Banking	
There should be a secure total protection policy / zero liability against loss for any customer induced transaction utilising technology through ATMs/ PoS/Online banking etc.	
A customer should not be made to be out of funds when any loss is suffered on account of Net/ATM banking transactions. All the rules in respect of internet banking should be so designed as to encourage consumers to feel safe about electronic transactions. In all the above scenarios, an immediate temporary credit, pending investigation, should be afforded.	
Banks have to necessarily ensure that all internet banking is made fail- safe by putting in place robust and dynamic fraud detection and prevention systems. Computerised / network delivery channels should have enhanced customer ease of operations and reduced costs for banks. Banks have to put in place fail-safe security systems for access, transactions etc. to increase the confidence of the bank customers to enable migration to electronic medium from conventional banking. The banks must ensure that the customers have the confidence in the systems that are being offered to them.	
The users (utilities, airlines, train tickets etc.) of electronic bank platforms for making collections should offer small discounts to their customers to favour electronic payments. This would result in substantial savings to them in cash management	
Banks may introduce mechanisms whereby a customer has a choice of restricting account to account transfers to be done only from particular IP addresses or a choice of addresses. A customer should also have the option of requesting blocking the transaction if the IP address is from a different	.

country. In fact, this should be the default option. Any change of option should be possible with ease through the call centre or online.	
Banks may restrict the amounts that can be transferred online by way of a day cap or by way of a ceiling amount per transfer. Additional factors of authentication should be taken and higher amounts should also be permitted for online transfers.	(i) Customer induced options may be provided for fixing a cap on the value / mode of transactions/beneficiaries. - In the event of customer wanting to exceed the cap, an additional authorization may be insisted upon. (ii)Limit on the number of beneficiaries that may be added in a day per account could be considered. (iii) A system of alert may be introduced when a beneficiary is added. (iv) Banks may put in place mechanism for velocity check on the number of transactions effected per day/ per beneficiary and any suspicious operations should be subjected to alert within the bank and to the customer
Banks may introduce systems whereby fund transfer facilities can be activated by the call centre on a need basis and deactivated once the transfer is completed. The facility should also be auto-closed (deactivation) after certain time (say 30 minutes).	
Banks in their systems should have facility of customer behavior/purchase pattern etc. analysis and any attempt from an unknown address / suspicious outlier debit transaction should be first blocked and then informed over SMS to the customer. The transaction should be allowed only after the customer authorises the transaction.	
Banks should put in place secure systems like multi-factor authentication to enhance customer confidence and reduce possibility of frauds	(v) The banks may consider implementation of digital signature for large value payments for all customers, to start with for RTGS transactions. (vi) Capturing of Internet Protocol (IP) address as an additional validation check should be considered.

The banks should have dynamic scoring models with inbuilt processes and controls to trigger transactions which are not normal so that even if the identity is stolen, the fraudster should not be in a position to succeed in his attempts. Study of customer transaction behavioral patterns and stopping irregular transactions should be part of the above process	
There must be multi-lateral arrangements amongst banks to deal with on-line banking frauds. Presently, there is lack of such an arrangement amongst banks and the customer is required to interact with different banks/ organisations when more than one bank / organisation is involved. The Indian Banks' Association (IBA) could provide such type of arrangements for all the banks.	(vii) Sub-membership of banks to the centralised payment systems has made it possible for the customers of such sub-members to reap the benefits of the same. Banks accepting sub-members should ensure that the security measures put in place by the sub members are on par with the standards followed by them so as to ensure the safety and mitigate the reputation risk.
It was felt that additional factors of authentication should be taken and higher amounts should also be permitted for online transfers as the present limits are seen to be restrictive for encouraging online money transfers.	(viii) Banks may explore the feasibility of implementing new technologies like adaptive authentication, etc. for fraud detection.
Banks should create customer access to banking for withdrawal of cash and for transactions by creating a chain of human ATM network of business correspondents of banks which will help enhance banking access all over the country. This is possible by hand held devices and mobile phones working online/offline with CBS systems of banks.	
Compensation	
The international best practices regarding cash not delivered at ATMs, withdrawal through cloned cards, credit card debits not authorised by customers, internet banking frauds etc., should be followed and the customer should be afforded a temporary credit immediately after taking a suitable undertaking.	
Further, the banks should facilitate early reporting of the above, by prescribing appropriate rules that will allow / provide a temporary credit which refunds the full amount, pending detailed investigation. The reporting timelines can also be linked with an	

amount which would act as the maximum customer liability. For instance, the maximum loss that a customer can suffer for a transaction reported within two working days should be capped at `10,000/-. This would mean that if a customer has been automatically credited the full amount on reporting a disputed transaction, after investigation into the matter has concluded, the maximum liability on the customer should not exceed `10,000/-. To cover the damages on refunds etc., banks should have insurance in place so that customer refunds are done in a hassle free manner without fear of losses. The electronic platforms have significantly reduced the operating costs for the banks and hence putting in place an appropriate insurance mechanism should be possible. The international best practices in this regard usually limit customer liability to a nominal amount if the issue is referred 60 days after occurrence.	
Card Transactions	
Issue of photo based cards - To avoid identity issues, all credit and debit cards (including chip cards) should be photo cards with the scanned signatures laminated on the card. Banks should also include the address of the card holder in the laminated portion to serve as a tool for KYC compliance for any other bank product. When UID is introduced, the cards issued thereafter should include the UID number also.	(i) All new debit and credit cards to be issued only for domestic usage - unless international use is specifically sought by the customer. -Such cards enabling international usage will have to be essentially EMV Chip and Pin enabled. (**By June 30, 2013**) (ii) Issuing banks should convert all existing MagStripe cards to EMV Chip card for all customers who have used their cards internationally at least once (for/through e-commerce/ATM/POS) (**By June 30, 2013**) (iii) All the active Magstripe international cards issued by banks should have threshold limit for international usage. The threshold should be determined by the banks based on the risk profile of the customer and accepted by the customer (**By**

	June 30, 2013). Till such time this process is completed an omnibus threshold limit (say, not exceeding USD 500) as determined by each bank may be put in place for all debit cards and all credit cards that have not been used for international transactions in the past. (iv) Banks should ensure that the terminals installed at the merchants for capturing card payments (including the double swipe terminals used) should be certified for PCI-DSS (Payment Card Industry- Data Security Standards) and PA-DSS (Payment Applications -Data Security Standards) (**By June 30, 2013**). (v) Bank should frame rules based on the transaction pattern of the usage of cards by the customers in coordination with the authorized card payment networks for arresting fraud. This would act as a fraud prevention measure (**By June 30, 2013**). (vi) Banks should ensure that all acquiring infrastructure that is currently operational on IP (Internet Protocol) based solutions are mandatorily made to go through PCI-DSS and PA-DSS certification. This should include acquirers, processors / aggregators and large merchants (**By June 30, 2013**). (vii) Banks should move towards real time fraud monitoring system at the earliest. (viii) Banks should provide easier methods (like SMS) for the customer to block his card and get a confirmation to that effect after

	blocking the card. (ix) Banks should move towards a system that facilitates implementation of additional factor of authentication for cards issued in India and used internationally (transactions acquired by banks located abroad). (x) Banks should build in a system of call referral in co-ordination with the card payment networks based on the rules framed at (v) above
Unique ID for every ATM – Every ATM should have a unique ID for reference. This would facilitate easy identification of the ATM when redressing the grievance. The ATM ID should appear on the transaction slip and also the bank statement.	
Blocking of ATM card – If an ATM card has been misused by another person, on receipt of SMS about use of the card, the customer should be able to immediately send return SMS to block the card (if he observes misuse) with a single word like 'BLOCK' to prevent further withdrawals (the SMS is being received from the mobile number registered with the bank). It is observed that considerable time is lost in locating the numbers of accounts, phone numbers etc., which gives the fraudsters more time to commit fraud.	
Further, in case of a lost card, hot-listing should be allowed online / over phone. However, a fresh debit card should not be allowed online / over phone by banks. The transaction in such cases should be automatically reversed and the amount should be credited back to the account (temporary credit). Even if auto-reversal does not happen, banks should pro-actively identify such cases and give charge-back.	

In case of doubt about the success / failure of an ATM transaction, the copy of the JP log is called for from an acquiring bank. The preceding and succeeding transactions should also be included in the copy.	
Chip based card (EMV): Banks should in a phased manner switch over to the use of chip based card (EMV) instead of the current magnetic strip based ones, in order to prevent skimming and damage / erosion of data due to wear and tear and misuse. This would accordingly entail necessary changes at all the front end machines like ATMs/PoS etc.	
As the switch over to chip based card would happen over a period of time, till the switch over is complete, the chip cards should as at present have a magnetic strip to enable transactions in the ATMs which have not switched over to chip cards.	
Merchant Discount / Fee for Debit Cards – To encourage acceptance of debit cards by the merchant establishments and thereby support electronic payments, card scheme providers and banks should follow a differential merchant fee policy in favour of debit/credit cards which will over a period of time reduce the dependence on cash for payments.	
Biometric ATM cards – Illiterate customers and senior citizens generally find it difficult to remember ATM-PIN. Banks may issue Biometric ATM cards to senior citizens and illiterate customers who are not at ease while using ordinary ATM cards. The necessary hardware changes at the front end devices may be made accordingly.	
ATM cards may be issued at the option of the customers on written request. Customers not desiring technology facilitation should not be forced to do so.	
Camera placement in ATMs – ATM cameras should be so placed as to take a clear picture of the person doing the ATM operations and the lighting inside the ATM booth should facilitate the same.	

An additional small camera should take a snapshot of the customer picking up the money from the bin so as to assist customers when cash disbursement does not take place. Whenever a complaint on ATM withdrawal is received, the bank should ensure to preserve the CCTV recordings till the grievance is fully redressed.	
The cash bin in ATMs may be so designed that the cash withdrawn falls into a bin which the customer picks up and this act should be recorded by the small camera	
PIN based authorisation – For debit / credit card transactions at the PoS,instead of signature based authorisation, PIN based authorisation should be made mandatory without any looping. There should be a phased withdrawal of non-pin based PoS machines.	
Two-Factor authentication for Internet Banking and Debit card transactions at PoS should be introduced. This will provide one additional layer of security.	
Additional factors like Grids etc., should not be printed on the back of the card but given separately so that a photocopy of the card does not give away all the information required for making an online payment.	
Mobile Banking	
Tiered security for different parameters: Transaction Value, Destination of transaction (two level authorisation for non-routine destinations), security based on hand-sets, frequency of payments should be introduced.	
All grievances of mobile banking should be addressed by the banks only without referring the customer to the service providers. The agreements of the banks with the telecom service providers should incorporate suitable provisions to address mobile banking grievances.	
Mobile banking coupled with digitisation of records can revolutionise everyday life for the vast majority. Economically weaker section shall be brought into the banking system by combining No Frills Account	

/ Micro Finance / Government subsidies and payments.	
At present, there is better penetration of post office and mobile telephony in rural areas. In immediate future post office accounts are to be linked with modern communication networks which can act as a platform for inter- operability of service providers like banks / MFIs, Mobile Network Operators and Mobile Application Providers.	
The ATM / PoS withdrawal using applications involving mobile phones is a more secure mode compared to withdrawal through bearer cheque as in this case both the parties viz. the account holder and the mobile owner are already subjected to full KYC and complete audit trail is available at both the ends. Hence, such transactions could be encouraged both at ATM as well as PoS up to the ceiling for withdrawal applicable for ATM and PoS respectively.	
Over the Limit Charges - The facility of 'over the limit' for credit card customers and that of simple overdraft for ATM card holders may be given on choice, the extent of over the limit/overdraft may be informed to the customer in advance and the charges for the same should not exceed the actual excess.	
Personalisation of accounts - Banks should design online programs on their sites enabling customers to automate money transfers, maintain balance levels, get non-standard account statements and a host of such facilities which would improve their information levels and make cash management more efficient.	
Self personalisation of Cards –	
Call centres as well as the online systems through net banking should enable a customer to: - Fix individual transaction limits for debit/credit card use. - Debar or fix limits for purchase of electronic or jewellery items. - Manipulate the limits for add on cards. - Activate/deactivate use of card internationally. - Limit the use of card to any particular state or a defined area.	

The above processes should be similar to electronic locking of STD or ISD facilities in telephone system and akin to international roaming in Cell Phones	
Banks should encourage formation of user communities to get feedback on the banks and also to enhance the efficiency of their products and design new products	
SMS Alerts	
Free SMS / e-mail alerts should be sent for every transaction such as date of maturity of deposit, ECS credit received, credit of pension, credit / receipt of money through RTGS etc.	
SMS alerts to be sent for all cheque returns irrespective of the amount or amount fixed at account level	
Account Statement in PDF format should be sent by e-mail, if customer requests so (password encrypted document).	
Current account holders with high transactions should be sent e-mail giving the balance position at agreed periodicity viz., daily, weekly, fortnightly etc.	
SMS alerts on card usage should be sent allowing the customer reply back in case card is not used.	
SMS or e-mail alert informing the change in interest rate on loan availed due to change in base rate etc.	
Compensation in-built in CBS	
The compensation that can be allowed for transaction deficiencies should be in-built into the CBS software and not left to the discretion of the branch staff.	
Systems should be in place to ensure automatic credit and there should be provision for double the credit in case a complaint is received.	
ECS Mandate Management System	
Bank should ensure that ECS Mandate Management System is working effectively to comply with the mandate given by the customer in respect of Limit of Debit amount, Expiry date, Withdrawal of Mandate, etc. Withdrawal of mandate for any ECS debit payment should not be left to the mercy of the beneficiary.	
Moving towards paperless fund transfers -	
Customers may be encouraged and given incentives to reduce cheque based transfers and migrate to other channels of fund transfers like NEFT, RTGS, ECS (debit/credit), Internet Banking and Mobile	

Banking. For the residual cheques in the system, cheque truncation should be implemented all over the country.	
Business Process Re-engineering -	
Banks should ensure that the CBS addresses the following major issues which were not integrated into CBS at the time of implementation in banks: -Automatic updation of age records and then conferring senior citizen benefits wherever applicable once a customer becomes a senior citizen. -Minor customer turning a major. -Cheques not being collected and honoured for the second account holder. -System not allowing the survivor to continue an either or survivor joint account after demise of one of the account holders. -System not allowing conversion of a single account to a joint account -Specialised Government Scheme accounts like PPF, Senior Citizen Special Deposit Schemes etc. not being updated in the system resulting in deposits being collected after expiry of schemes. -Tax deducted at source not being communicated to the IT department for appropriate credit to assessee accounts. -Tax deducted at source even after collection Form 15 G, 15 H etc., registering and issuance of acknowledgements to the account holders in respect of nominees. -Diarisation for receipt and reminder of Life Certificate for pensioners	