ATM Transactions in Banks: Major Security Concerns

Speaking at a recent function in Hyderabad, the Reserve Bank of India Governor, Dr D. Subbarao, has sounded a warning to bankers highlighting the need to ensure that technology does not become a barrier between customers and bankers. ‘‘Faceless banking can be intimidating…" said the Governor, adding that technology cannot substitute brick and mortar branches.

The advent of technology has changed the face of banking in the country today. The moment we say bank, people in 40’s and 50’s would recollect a brick and mortar structure with a cash cabin, a manager’s cabin and a few subordinate staff walking here and there with ledgers and registers in hand. But when you say ‘bank’ to a youth in 20’s he will think of a faceless machine, an ATM or a computer that takes his user-id and his personal password (or a PIN) and prompts him to enter his transaction. Though intimidating, the stark reality is that we are all heading for a faceless banking, a computer-driven service, an electronic delivery system. Thus, an electronic delivery channel in a bank is the delivery of customer service through an electronic device as against a person sitting at the counter and delivering the service like a normal cash disbursement.

ATM’s, e-banking, Mobile Banking and **Credit/Debit Card** Services are all part of electronic delivery channels of banks. Let us now see some of the major security concerns in these channels. Let us start with ATM’s, being the most popular among such delivery channels.

ATM’s are of two types from connectivity point of view: **Online ATM’s and Off-line** ATM’s. Typically, all ATM’s should be online which means they are connected to the server (mostly the CBS online server) and the transaction like cash withdrawal is updated in the database and in the customer’s account online and then only the cash is disbursed. In the case of offline ATM, there is no such connectivity, which quite often, may be a temporary feature too.

From location point of view, ATM’s can be **on-site ATM** or an **off-Site ATM.** An off-site ATM is one which is not part of the branch premises and is not connected to the branch in its LAN (Local Area Network). An on-site ATM is normally well inside the branch premises and is connected to the branch by its LAN. Interestingly, if an ATM is just across the road (on the opposite side) and hence is not part of the branch LAN, it would still be an onsite ATM, even if is actually closer to the branch than one which is a few buildings away but still within the branch LAN and inside the same building complex.

Security risks to an ATM may be viewed broadly from two angles viz Physical Security Risks and Logical (Software) Security Risks.

Some of the most common physical security risks are as follows:

- Theft of an ATM,
- Sabotage,
- Damage to ATM and its peripherals,
- Loss or theft of information assets inside the ATM or in the cabin etc.

All these are threats to the actual cash kept inside the ATM. Besides these, there are also some perceived threats to the customers at the ATM cabins which also come under the category of physical risks. Some of these include **shoulder surfing** (looking through the shoulder, at the ATM PIN while it is entered), **social engineering** (befriending the customer and getting his PIN), physical attack to the customer especially at night in or near an off-site ATM, stealing the ATM card and the pouch or purse or even the mobile where the ATM PIN is recorded (written) by the owner.

Solutions to such physical security concerns lie basically in not revealing the ATM PIN to any one, repeat any one, and not writing it anywhere, absolutely ANYWHERE, not even in the purse or a diary or in notepad and other documents in the laptop. Even till recently, there were many cases of purses and pouches getting pick-pocketed in which the ATM cards are kept, where the owner has written the PIN also in a separate piece of paper. Thanks to the awareness spread by banks and users about the use of ATMs and PINs, of late, such cases (of writing the PIN number in a paper and keeping it in the same purse where the ATM Card is kept) have become quite rare.

On the software side, it is now mandated, as per international standards, that all ATM's are enabled with 128-bit encryption which in normal parlance means that the ATM transactions are **communicated in an encrypted manner through a secure channel** and cannot be tapped or intercepted or manipulated by any intruder in that communication channel. All banks conform to the standards stipulated by Visa and Master the two leading players in the field.

Banks have enormous responsibility to ensure proper security and to prevent ATM related frauds. Card Management is itself a complex and mammoth task. Banks now ensure that ATM Cards and the PIN Mailer are both not sent directly to the customer and never by the same courier or post. If the PIN Mailer is generated by the Card Management agency and sent directly to the customer, then the ATM card is delivered to him/her at the branch. To avoid delay and to ensure delivery of ATMs and PIN Mailer on the date of opening of account, as a marketing strategy, banks also give non personalised card along with the PIN Mailer directly to the customer immediately after the account is opened. In such cases, custody of such ATM Cards and PIN Mailers is of paramount concern on the part of banks.

Dealing with **captured ATM Cards, confiscated card, surrendered cards** (on the closure of accounts) is also a serious concern. Unless properly documented as a procedure and ensuring compliance to such procedures, card management poses serious operational risk and provides dangerous scope for fraudsters inside the bank trapping in the process, gullible and innocent bank officials too. Unscrupulous and evil-minded, though rarest of the rare in the industry, have a field day in dealing with customers who come with ATM complaints and surrender their cards. Banks should ensure to have proper procedures in place to acknowledge receipt of any ATM Card with date and time, destroy the card physically in the presence of the customer against his/her acknowledgement and all related well laid down procedures.

Outsourced Card Management is another major issue. Whenever card issue is outsourced, banks should ensure that responsibility is clearly fixed on the firm to whom the services are outsourced and that all scenarios and eventualities are taken care of at the time of drafting of Service Level Agreement. Most of the banks nowadays have outsourced not only card management but also physical maintenance of ATM's. In any case of outsourcing, the biggest precaution banks should take is with regard to the terms and conditions of Service Level Agreement. Not just with regard to cleanliness of ATM cabins, the vendors are to take care of physical maintenance of ATM cabins, physical access control at the door, provision of security guards etc. Whenever cash loading and cash management of ATM's is also involved, care should be taken to ensure that cash inside the ATM cassettes are properly accounted for, only genuine and clean notes are kept, no counterfeit notes are kept etc.

With the concept of ATM consortiums like CashTree and NFS now gone and with the facility to draw from any ATM for any card, the problem of inter-bank payments and the resultant reconciliation issues pose a major concern. **ATM Logs and transaction trails** play a major role in solving such disputes. Through RBI in its directives has said that any inter-bank ATM reconciliation (arising out of dispute of account debited but cash not paid etc) should be solved within 12 days and the concerned bank should pay a penalty of Rs.100/- per day for every subsequent day of non-settlement, in practice banks find it very difficult to address these issues. Inter-bank reconciliation thus is a major area that needs to be addressed by every bank preferably by deploying dedicated team of officials at the corporate level.

In the event of any legal disputes arising out of ATM frauds, inter-bank reconciliation issues etc the logs and trails maintained at the ATM Switch level (ie the main server centrally controlling all ATM transactions) play a significant role as evidence. **Such e-records are legally accepted** as evidences and banks have to prove that maintaining such e-records and producing a print-out of the same are valid evidences subject to the fulfilling criteria mentioned in the Bankers Book Evidence Act, as amended by the I.T. Act 2000. With legal recognition given to e-records there is much more responsibility on the part of banks to prove that the norms given in the Act have been adhered to.

Besides, more so with the amendment to the **IT Act 2000** vide **IT Amendment Act 2008** and with the introduction of Sec 43-A, banks as custodians of customers data are now bound to maintain 'reasonable security practices' as described in detail in the Section and failure to maintain the same will make the body corporate liable to pay damages by way of compensation to the person affected.

Much lies on the part of users being the public account holders to ensure that ATM frauds are prevented. ATM PIN should never be written anywhere nor divulged to anyone. ATM card should never be parted with. Many pensioners and senior citizens taking ATM Cards but not comfortable in drawing from ATM's, are in the habit of handing over the cards to their sons and daughters telling them to operate at the ATM's who as adolescents may not know the seriousness. Sometimes banks too are to blame for such a scenario since, in their anxiety to market ATM cards they give them to those who do not know the fundamentals, or give non-personalised cards sometimes even when not demanded. In a free, open and globalised industry such competition among banks is not only understandable but also desirable. However, of late, banks do also take initiatives to spread awareness on the use of ATM's as well as the awareness about the usage, mis-use etc.

Banks have a greater role to play in the security of an ATM transaction. Banks are to ensure that the PIN when being typed cannot be noticed by any one ensuring the design and layout of the ATM cabin provides adequate security to the customer when he is typing the PIN. Banks have to provide for security guards in all the ATM's ensuring

As technology keeps progressing, so are the initiatives taken by banks to keep the customers money safe and to keep its information assets safe. Normally the fraudsters are always one step ahead of the investigators and this is more so in the case of technological crimes. In the case of cyber crimes like ATM offences, most often, the criminals know the nuances much earlier and use it to their advantage in committing a crime and only later do the police come to know of the technology involved.

To conclude, safe and secure ATM banking involves significant roles from three main players viz the Regulators (like RBI etc), the Service Providers (banks etc) and the users (customers). Much is to be done on the part of regulators too in formulating uniform guidelines for inspection of ATM transactions, IS Audit of ATM related areas, ensuring adherence to 'reasonable security practices' by banks etc.

****.****

Author: V. Rajendran, Cyber Law Consultant
91+44+22473849; 91+9444073849
Email: venkat.rajen@gmail.com, venkrajen@yahoo.com