ATM POLICY

For

SUNDARLALJI SAWJEE URBAN CO-OPERATIVE BANK LTD

Content

1. INTRODUCTION

- SUNDARLALJI SAWJEE UBRAN CO-OPERATIVE BANK LTD was Founded in …….. is serving for its customers on various channels. Being top bank in Co-Operative section, BANK is providing its customers advance services and features.

- In the age of electronic and mobile devices banking sector has shown a tremendous growth. BANK has also taken various initiatives in order to keep in competition with growing banks.
- Today, almost every commercial bank branch is at some stage of technology adoption: core banking solution (CBS), or alternate delivery channels such as internet banking, mobile banking, phone banking and ATMs. Hence with emerging technology there arises a need of security, in terms of finance, data and other aspects of information.

2. OBJECTIVE:-

- To achieve safe, sound and resilient ATM network and cash flow biding with the technological standards mentioned as per RBI and ITA 2000 and ITAA and other governing laws.
- This document identifies security guidelines for ATMs, considering the protection that can be provided by the hardware and the software of the ATM itself against attacks aimed at compromising sensitive data acquired, stored, exported, or in any way processed by the device.
- Intended Audience
- The Policy is formulated for the IT department and or the Banking cell taking in or working for the ATM related services

3. SCOPE:

- This policy document covers the implementation of new features , operations , roles and responsibilities in ATM channel and services.

4. RESPONSIBILITY

- The Admin officials are responsible for approval and execution of the ATM Policy. The time of review of policy and the management of the same will be taken care by Admin.

5. OVERSIGHT AND PUBLIC POLICY GOALS

- The Bank monitors and review ATM services from time to time and ensure that:
  i. The legal and regulatory environment is appropriate and keeps pace with domestic and international developments;
  ii. Market structure remains satisfactory and the markets are functioning adequately with healthy competition among service providers;
  iii. International standards are complied with in respect of infrastructures and cards to reduce risk and increase safety and efficiency; and
  iv. The provision of services by the central bank is fair and based on objective criteria.

6. MANAGEMENT RISK ANALYSIS:

- Bank has been following and implemented the process of identifying, measuring, monitoring and managing all potential risk in ATM transactions.
- Bank is identifying, monitoring and keep track report of the following on regular basis.

  i. Total no. of active ATMs

  ii. Time Logged on/ Settlement time.

  iii. Number of Cardholders.

  iv. Number of transactions i.e. withdrawals and transfers

v. Total amount transacted through withdrawals and transfers.

vi. Number of ATM generated reports.

vii. Evaluating and inspecting transaction processing, System administration.

viii. Identifying the Risk Areas.

ix. ATM internal process and services.

x. Internal Infrastructure Risks.

xi. Operations of ATM channel.

xii. Legal Risk.

xiii. Overall review of ATM management resources.

xiv. Incident Management.

xv. Risk Management.

7. ATM RISK MANAGEMENT:

BANK would review the risk and monitor ATM services by following below mentioned aspects:

- Review the existing ATM environment on regular basis,
- Identify the critical information processing of ATM applications,
- Monitoring and checking that all ATM should be equipped with mechanism preventing skimming attacks,
- Applied mechanism to monitor that each ATM is equipped with only one card holder interface,
- Continues surveillance on all ATM that they are equipped with security Cameras,
- Take all necessary steps to protect ATM assets and Application,

- Managing and identifying various hazards to which ATM centers that may exposed including natural disaster or otherwise,
- Identifying the controls that are in operation to reduce possible impacts of threats/risks,
- Following all the security controls and guidelines suggested by PCI DSS,
- Monitoring an Intrusion Detection System that must be configured to monitor all traffic and alert on any abnormal behavior,
- Firewall should be configured and be kept up to date and should allow only known application traffic inward and outward,
- Patch management program for ATM operating system and applications should be in place to ensure ATM software is well patched,
- Software Whitelisting solution for ATMs and it should be in place and an anti-virus must be installed and always updated,
- Develop an incident management system and an incident response plan prepared for rapid deployment in case of a compromise. This is to ensure ATM frauds are reported in real time,
- ATM software must be updated regularly,
- ATM operators should migrate to EMV chip and pin card and should eliminate magnetic stripe fall back. This will mitigate the risk of skimming cards,
- Segregation of ATM network from the rest of the bank's network by using a firewall and virtual local area networks,
- ATM PC BIOS must be secured,
- A password policy must be in place to ensure only strong passwords are used on ATMs and each user has their own unique password,
- All communications on the ATMs that is encrypted including communication between the PC core and the cash dispenser,

- All unused services and applications must be removed from the ATM to reduce the attack surface,
- Deploys effective anti-malware software and hardened PC core operating system,
- Implementing a role based access control on the ATM environment,
- Penetration testing must be done on the ATM annually,
- Ensuring ATM physical security like CCTV and alarms when installing the ATM,
- Installation of tool that will ensure the ATM's confidentiality, Integrity and availability,
- Determine whether the necessary controls are in place periodically,

8. TYPES OF ERRORS

Bank have management/handling plan for the following errors can occur due to mechanical failure at the ATM terminal:

i. ATM dispenses less cash to the customer but the amount is debited correctly

ii. The customer's account is debited twice but the cash is only dispensed once by ATM

iii. The Customer's account is debited but cash is not dispensed by ATM

9. ATM SECURITY MEASURES:

- **The ATM Audit Log**

  Record and track of ATM audit Log that provides recorded information after incident.

- **Encryption**

  All ATM system installed are encrypted and updated time to time.

- **Software Audit**

  Perform software audit of all installed and active ATMs to analyze the ATM operations.

  Monitoring operations of ATMs and detect possible tampering with the programs.

  Perform audit to detect that program are being properly executed and not being over-ridden or bypassed.

10. CONTROLS

This requirement should be addressed with the controls implemented at different levels of ATM implementation, such as General Application Control, Business Process Control, and Application Process Control, CIA Controls.

- **General ATM operation and Organizational Controls:**

The operation and organizational controls must be segregated among the individuals, There are two main important elements in an ATM systems; firstly the magnetic card and secondly PINs. Segregation of duties shall be maintained by assuring that making of the PINs is not to be carried out by people who are processing the cards.

Following segregation is to be followed by Bank:

- Application testing from systems design and programming
- System software programming from Application programming

- **Business Process Controls**

Bank personnel having access to cards must be denied access to PINs whenever the cards are prepared and processed. Bank takes care of segregation of duties that no one person shall handle all the transaction. Bank makes sure that.

11. ATM TECHNOLOGICAL STANDARDS AND SECURITY MEASURES :

Bank has established secured network and implemented security measures for mitigating risk in ATM operations, which are listed as below:

a) All ATMs shall be operated for cash replenishment only with digital One Time Combination (OTC) locks.

b) All ATMs shall be grouted to a structure (wall, pillar, floor, etc.), except for ATMs installed in highly secured premises such as airports, etc. which have adequate CCTV coverage and are guarded by state / central security personnel.

c) Bank also rolling out a comprehensive e-surveillance mechanism at the ATMs to ensure timely alerts and quick response.

- **Monitoring**

The following scope is inclusive of problem determination and resolution tasks which Bank is considering for central management of ATMs, all of which can be performed remotely with good ATM monitoring and management tools:

a) Gracefully reboot the ATM; allow current transactions to finish before rebooting!

b) Retrieve log files and security events.

c) Retrieve performance information about memory, disk space, CPU usage, process lists, network ports, etc.

d) Restart critical services on the ATM.

e) Log all of the verification information available to local service personnel using the supervisor panel.

f) Validate and enforce security tools and policies.

- **Integration**

Management and security tools that Bank has been used successfully in ATM systems which are mentioned below:

- Central authentication of user accounts used at the ATM.
- Inventory systems to track information about ATM hardware and software.
- Multi-factor authentication implementations for administrative access that use a token or similar device as part of authentication.
- Network monitoring systems to analyze the network performance of the ATMs.

- **Cryptographic Key Management for ATMs**

Bank applies key management process which is associated with financial transactions and for encrypting PIN Pad. The very essence of protection in an encrypted environment is the secrecy of the key.

- **Firewalls and Network Isolation**

Bank has installed software based firewall protection which has been the most security measure as it cannot be compromised through physical access alone.

Bank has established effective network isolation and intrusion detection/ risk mitigation tools. Bank uses network isolation or network encryption techniques to ensure that cardholder data cannot travel outside the ATM system itself. Bank has a good core set of layered security which involves network isolation, tested operating system hardening, secure operating processes, and central monitoring/management tools.

12. SECURITY AND CONTROL OF PIN (PERSONAL IDENTIFICATION NUMBER)

PINs are stored in encrypted form and should be stored in database file for security purposes. The PIN mailers are prepared separately and also bank has taken necessary actions to check that PIN is not being misused by any Bank employee. Bank ensures that Pin is activated only upon the use of card by the customer at the ATM.

For security and confidentiality reasons all systems documentation concerning PIN generation/encryption and decryption key must be under 3D level security controls all time.

- **Bank is implementing controls while providing ATM services are mentioned as below:**

i. PIN mailers should not have direct access to the customer's account number or any account related information.

ii. Access controls and authorization to any addition, deletion or changes to ATM transaction details should be implemented

iii. Any changes to cardholder details should be authorized by the officer at the next level.

iv. Realistic maximum transaction and maximum daily total limits should be implemented for ATM withdrawals.

v. Printed receipts should be dispensed by the ATM for every ATM transaction.

vi. Every ATM transaction should be acknowledged by e-mail or short message script sent to the mobile phone to confirm or alert the user that a transaction was performed.

13. APPLICATION CONTROL AND SECURITY:

There are well-known information systems security issues associated with applications software, whether the software is developed internally or acquired from an external source. Attackers can potentially use many different paths through the application to do harm to the business. To determine the risk to itself, Bank has been evaluating the likelihood associated with the threat agent, attack vector and security weakness and combines it with an estimate of the technical and business impact to the organization. Together, these factors determine the overall risk.

The following are the important Application control and risk mitigation measures are implemented by Bank:

1. Each application has an owner which will typically be the concerned business function that uses the application

2. Some of the roles of application owners include:

- Prioritizing any changes to be made to the application and authorizing the changes
- Deciding on data classification/de-classification and archival/purging procedures for the data pertaining to an application as per relevant policies/regulatory/statutory requirements
- Ensuring that adequate controls are built into the application through active involvement in the application design, development, testing and change process
- Ensuring that the application meets the business/functional needs of the users
- Ensuring that the information security function has reviewed the security of the application
- Taking decisions on any new applications to be acquired / developed or any old applications to be discarded
- Informing the information security team regarding purchase of an application and assessing the application based on the security policy requirements

- Ensuring that the Change Management process is followed for any changes in application
- Ensuring that the new applications being purchased/developed follow the Information Security policy
- Ensuring that logs or audit trails, as required, are enabled and monitored for the applications
- All application systems are tested before implementation in a robust manner regarding controls to ensure that they satisfy business policies/rules of the bank and regulatory and legal prescriptions/requirements. Before the system is live, clarity on the audit trails and the specific fields that are required are captured as part of audit trails and an audit trail or log monitoring process including personnel responsible for the same.
- Bank incorporates information security at all stages of software development. This would assist in improving software quality and minimizing exposure to vulnerabilities. Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, security event tracking and exception handling are required to be clearly specified at the initial stages of system development/acquisition. A compliance check against the bank's security standards and regulatory/statutory requirements is also done.
- All application systems have audit trails along with policy/procedure of log monitoring for such systems including the clear allocation of responsibility in this regard. Every application affecting critical/sensitive information, for example, impacting financial, customer, control, regulatory and legal aspects, provides for detailed audit trails/ logging capability with details like transaction id, date, time, originator id, authorizer id, actions undertaken by a given user id, etc. Other details like logging the IP address of the client machine, terminal identity or location may also be considered.
- Applications also provide for, inter-alia; logging unsuccessful logon attempts, access to sensitive options in the application, e.g., master record changes,

granting of access rights, use of system utilities, changes in system configuration, etc.

- The audit trails are stored as per a defined period as per any internal/regulatory/statutory requirements and it are ensured that they are not tampered with.
- There are documented standards/procedures for administering the application, which are approved by the application owner and kept up-to-date.
- The development, test and production environments are properly segregated.
- Access is based on the principle of least privilege and "need to know" commensurate with the job responsibilities. Adequate segregation of duties is enforced.
- There are controls on updating key 'static' business information like customer master files, parameter changes, etc.
- Any changes to an application system/data are justified by genuine business need and approvals supported by documentation and subjected to a robust change management process. The change management would involve generating a request, risk assessment, authorization from an appropriate authority, implementation, testing and verification of the change done.
- Potential security weaknesses / breaches (for example, as a result of analyzing user behavior or patterns of network traffic) are always identified.
- There are appropriate measures to reduce the risk of theft, fraud, error and unauthorized changes to information through measures like supervision of activities and segregation of duties.
- Applications do not allow unauthorized entries to be updated in the database. Similarly, applications do not allow any modifications to be made after an entry is authorized. Any subsequent changes are made only by reversing the original authorized entry and passing a fresh entry.

- Direct back-end updates to database not be allowed except during exigencies, with a clear business need and after due authorization as per the relevant policy.
- Access to the database prompt is restricted only to the database administrator.
- Robust input validation controls, processing and output controls are built in to the application.
- Alerts regarding use of the same machine for both maker and checker transactions are considered.
- Error / exception reports and logs are reviewed and any issue is remedied /addressed at the earliest.
- Critical functions or applications dealing with financial, regulatory and legal, MIS and risk assessment/management, (for example, calculation of capital adequacy, ALM, calculating Vary, risk weighted assets, NPA classification and provisioning, balance sheet compilation, AML system, revaluation of foreign currency balances, computation of MTM gains / losses, etc.,) is done through proper application systems and not manually or in a semi-automated manner through spreadsheets. These pose risks relating to data integrity and reliability. Use of spreadsheets in this regard is restricted and is replaced by appropriate IT applications within a definite timeframe in a phased manner.
- Bank obtains application integrity statements in writing from the application system vendors providing for reasonable level of assurance about the application being free of malware at the time of sale, free of any obvious bugs, and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done).
- For all critical applications, either the source code is received from the vendor or a software escrow agreement which is in place with a third party to ensure source code availability in the event the vendor goes out of business. It is ensured that product updates and programme fixes are also included in the escrow agreement.

- Applications are configured to logout the users after a specific period of inactivity. The application ensures rollover of incomplete transactions and otherwise ensures integrity of data in case of a log out.

- There are suitable interface controls in place. Data transfer from one process to another or from one application to another, particularly for critical systems, not has any manual intervention in order to prevent any unauthorized modification. The process are automated and properly integrated with due authentication mechanism and audit trails by enabling "Straight Through Processing" between applications or from data sources to replace any manual intervention/semi-automated processes like extracting data in text files and uploading to the target system, importing to a spreadsheet, etc. Further, proper validations and reconciliation of data is carried out between relevant interfaces/applications across the bank. The bank suitably integrates the systems and applications, as required, to enhance data integrity and reliability.

- Multi-tier application architecture are considered for relevant critical systems like internet banking systems which differentiate session control, presentation logic, server side input validation, business logic and database access.

- In the event of data pertaining to Indian operations being stored and/or processed abroad, for example, by foreign Bank, there are suitable controls like segregation of data and strict access controls based on 'need to know' and robust change controls. The bank is in a position to adequately prove the same to the regulator. Regulator's access to such data/records and other relevant information is not impeded in any manner and RBI would have the right to cause an inspection to be made of the processing centre/data centre and its books and accounts by one or more of its officers or employees or other persons.

- An application security review/testing, initially and during major changes, are conducted using a combination of source code review, stress loading, exception testing and compliance review to identify insecure coding techniques and systems vulnerabilities to a reasonable extent.

- Critical application system logs/audit trails also is backed up as part of the application backup policy.

- Robust System Security Testing, in respect of critical e-banking systems, incorporate, inter-alia, specifications relating to information leakage, business logic, authentication, authorization, input data validation, exception/error handling, session management, cryptography and detailed logging, as relevant. These is carried out at least on annual basis

14. GENERAL INFORMATION REGARDING DELIVERY CHANNELS

- Provision of various electronic banking channels like ATM/debit cards/internet banking/phone banking are issued only at the option of the customers based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions from the customer. Customer is not being forced to opt for services in this regard. Bank provides clear information to their customers about the risks and benefits of using e-banking delivery services to enable customers to decide on choosing such services.
- When new operating features or functions, particularly those relating to security, integrity and authentication, are being introduced, the bank ensure that the customers have sufficient instruction and information to be able to properly utilize them.
- To raise security awareness, Bank sensitizes customers on the need to protect their PINs, security tokens, personal details and other confidential data.
- Bank is responsible for the safety and soundness of the services and systems they provide to their customers. Reciprocally, it is also important that customers take appropriate security measures to protect their devices and computer systems and ensure that their integrity is not compromised when engaging in online banking. Customers implement the measures advised by their Bank regarding protecting their devices or computers which they use for accessing banking services.
- In view of the constant changes occurring in the internet environment and online delivery channels, management institute a risk monitoring and

compliance regime on an ongoing basis to ascertain the performance and effectiveness of the risk management process. When risk parameters change, the risk process are updated and enhanced accordingly. Re-evaluation of past risk-control measures and equations, renewed testing and auditing of the adequacy and effectiveness of the risk management process and the attendant controls and security measures taken are conducted.

15. PROTOCOL SECURITY ANALYSIS

- Bank is implementing security properties required by ATM systems must include confidentiality, authentication, integrity and non-repudiation. Confidentiality confidentially means guaranteeing data and important user information not to be accessed by unauthorized users and aliens that usually is performed using cryptography techniques.
- Bank uses encryption to communicate and sharing any confidential information to establish confidentiality in the communication. Integrity is needed to prevent and discover redundancy, modification, and deletion of data. While registering an ATM and a user in a bank, two independent certificates are issued for these two entities. Both certificates are signed by the user. To establish integrity, Bank uses digital signature in the protocol communication. Non-Repudiation prevents the sender from denying the transmission of message. Bank has created this mechanism using the signature in the scenario. Since all the signatures in our protocol use private key of the sender, nobody can repudiates the message that has been sent before.

16. CUSTOMER AWARENESS ON FRAUDS

- **CREATION OF CUSTOMER AWARENESS ON FRAUDS**

1. Customer awareness is one of the pillars of fraud prevention. It has been seen that alert customers have enabled prevention of several frauds and in case of frauds which could not be avoided, helped in bringing the culprit to book by raising timely alerts. Bank thus aim at continuously educating its customers and solicit their participation in various preventive/detective measures. It is the duty of all the groups in Bank to create fraud risk awareness amongst their respective

customers. The fraud risk management group shares its understanding of frauds with each group, identify areas where customer awareness is lacking and if required, guide the groups on programmes to be run for creation of awareness amongst customers. The groups ensure that in each of their interaction with customers there is at least one message to make the customer aware of fraud risk.

2. The following are some of the recommended measures to create awareness amongst customers:

   - Publications in leading newspapers
   - Detailed 'do's and don'ts' on the web site of the bank
   - Messages along with statement of accounts, either physical or online
   - Messages printed on bank's stationery such as envelopes, card covers, etc.
   - SMS /Email alerts for security tips(OTP/CVV/PIN/CARD/Transaction alerts Message) on phone banking when the customer calls
   - As inserts or on the jackets of cheque books
   - Posters in branches and ATM centers
   - Interstitials on television and radio

3. It is ensured that the communication to the customer is simple and aimed at making them aware of fraud risks and seeking their involvement in taking proper precautions aimed at preventing frauds. Such communication is reviewed periodically by the fraud risk management group to judge its effectiveness.

17. EMPLOYEE AWARENESS AND TRAINING

1. Employee awareness is crucial to fraud prevention. Training on fraud prevention practices are provided by the fraud risk management group at various forums.

2. Bank uses the following methods to create employee awareness:

- Class room training programs at the time of induction or during risk related training sessions
- Publication of newsletters on frauds covering various aspects of frauds and containing important message on fraud prevention from senior functionaries of the Bank
- E-learning module on fraud prevention
- Online games based on fraud risks in specific products or processes
- E-tests on prevention practices and controls
- Detailed 'do's and don'ts' put up on the worksite of the employee
- Safety tips flashed at the time of logging into Core Banking System (CBS), screen savers, etc.
- Emails sent by the respective business heads
- Posters on various safety measures at the work place
- Messages/discussions during daily work huddles

18. THREATS TO ATM NETWORKS

As other networks, ATM networks will suffer a lot of threats. ATM threats/attacks can be divided into physical and logical attacks. Physical attacks involve attacking the ATM physically like exploding the ATM safe to have access to the ATM safe money. In physical attack, cyber criminals use methods such as solid and gas explosives, as well as uprooting the ATM from the site and then using other method to get access to safe and secure network. Other physical attack involves placing gadgets to ATM by cyber criminals that copy ATM card data and reproduce it on another blank card that can be used to perform unauthorized transaction from cardholder's account. Logical attacks includes malware attacks to instruct ATM to perform the transaction. This attack can be achieved by gaining physical access on the ATM in order to

install malware on the system or it can be injected using network. Types of attacks on ATM network are as follows:

- **ATM Card Skimming Attacks**

ATM card skimming attack is a physical threat which has been the number one ATM threat globally in the past. ATM skimming refers to the stealing of the electronic card data, aiding the criminal to counterfeit the card. A skimmer is a device that is installed on a card reader making a customer believe they are inserting their card in a ATM card reader. The skimmer reads the data from a card's magnetic stripe or EMV chip when a client inserts a card into the ATM. Some skimmers have the capability to read data from an EMV card chip at a distance. ATM skimming attacks are however on the decrease due to deployment of anti-skimming solutions, payment card industry data security standard (PCI DSS), EMV technology and contactless ATM functionality. Customers are unable to notice a problem and experience a normal ATM transaction until their account is defrauded. The most common places where skimmers are placed on the ATM. Multifactor authentication using biometrics can be used as an added security mechanism against this type of fraud.

- **Eavesdropping Skimming Attack**

A new type of skimming attack called Eavesdropping Skimming has emerged and expanded predominantly in the world. The attack targets ATM motorized card readers on older model of ATM called personas. The attacker penetrates the ATM facial to have access to the card Reader of the ATM. A skimmer is then fitted directly onto an electrical node that carries card data on the card reader. On Personas ATMs, the attacker targets the card reader electronic control board by creating a hole behind the ATM card orientation window. In the newer attacks against ATMs, the attacker has changed the method but has maintained the principle. The variance in the way this attack is performed on the two different ATM series shows how sophisticated ATM cyber-criminals are.

- **ATM Card Shimming Attack**

ATM card shimming attack is a Man-in-the-Middle attack in which the cyber-criminal inserts a device into the ATM card reader that intercepts and records the data flowing between the EMV chip and the ATM card reader . This data

could then possibly be reused to clone a magnetic stripe card. EMV chip data and magnetic stripe data have different check values (CVVs) and therefore the data that is captured from the EMV chip card can't be used to clone a magnetic stripe. Card Shimming is neither vulnerability with a chip card, nor with an ATM. It is therefore not necessary to add protection mechanisms against this form of attack to the ATM. If the proper authorization procedure is followed during an ATM transaction, counterfeit cards can be immediately detected. This attack can only be successful if an issuer neglects to check the CVV when authorizing a transaction. All issuers must therefore make these basic checks to prevent this category of fraud.

- **ATM Card Trapping Attack**

ATM Card Trapping steals the physical card itself through a device attached to the ATM. Cyber-criminals place a device directly over or into an ATM's card reader slot. These devices are designed to capture cards after customers' insert them. In a magnetic stripe environment or chip-and-signature environment, the PIN does not need to be compromised and therefore having an ATM is enough to compromise a customer's account.

- ***ATM Cash Trapping Attack***

Cash trapping is where the cyber-criminal uses a device to physically trap the cash that is dispensed and comes to collect it once the customer has left the ATM location. This fraud involves placement of money traps or false presenters in front of the ATM dispenser. When processing a transaction, an ATM dispenses notes into the trap set by cyber-criminals rather than present the money to the customer. The customer assumes the ATM has malfunctioned and leaves. The cyber-criminal then returns, removes the money trap or false presenter, and leaves with cash that was intended for the customer. Cash trapping however mostly succeeds with insider involvement. ATM owners must put measures in place that helps mitigate insider threats.

- **Transaction Reversal Fraud**

Transaction Reversal Fraud (TRF) involves the creation of an error that makes it appear as though the cash has not been dispensed. The account is re-credited the amount 'withdrawn' but the criminal pockets the money. It could be a physical grab (similar to cash trapping) or a corruption of the transaction

message. The attacker achieves this by creating a fault on the ATM during a cash dispense operation causing the host switch to reverse the transaction. The account will not be debited although the criminal will remove the cash from the ATM. To avoid being caught, attackers use stolen or skimmed cards. The attacker causes an error on the card reader during cash dispense operation. The correct PIN is entered and cash requested. After the transaction is authorized by the host switch, the ATM counts the cash and positions it behind the cash dispenser shutter waiting to be dispensed. The card is ejected and the attacker waits for the ATM transaction to time out and attempt to capture the card. At this point the attacker holds the card and prevents it from being captured and then forces the cash dispenser shutter open and removes the stacked cash. The ATM reports a card jam and reverses the transaction.

- **Social Engineering/Phishing Attacks**

The Victim is tricked into revealing his/her authentication information (PIN). It can be physically or through electronic means. e.g., rogue websites are set up by the perpetrators to collect authentication information from un-suspecting customers in the name of necessary updates or changes being carried out by their 'Bankers'. The user ends up divulging his card sensitive data to the rogue site.

- **Operational Fraud**

The ATM dispenser is manipulated in this type of fraud. The ATM is configured to dispense big denominations as smaller ones, there-by giving out more money than should be dispensed. This can be achieved by either loading wrong denomination notes in the wrong money cassettes or by making a wrong configuration in the software.

- **Malware Attacks**

Malware attacks are usually easier with insider involvement as physical access is necessary to deploy the virus. However, this attack is possible online today. The malware file or device is placed on the ATM; its control device is then triggered to give remote control to the perpetrator through a custom interface which enables capture of card numbers and PINs through the private memory space of transaction-processing applications installed on a compromised ATM.

Magnetic stripe cards are very vulnerable to this type of attack. Deployment of effective anti-malware software can help mitigate this class of attacks.

- **Man-in-the-Middle Attack**

This class of attack occurs when malware is placed within the banks network and compromises the banks network infrastructure. The network traffic is monitored and the malware listens for transaction messages from the ATMs

When the malware recognizes a cash withdrawal transaction message from a bank card, it intercepts the corresponding host response from the ATM switch and changes the authorized dispense amount to a larger sum than requested and approved by the ATM switch. In order to perform the fraud, an attacker will initiate a withdrawal transaction at any ATM on the compromised bank network. The attacker will use a pre-defined known card number. The transaction will be intercepted and the card number will be recognized by the malware. It will then wait for the host response to the withdrawal request. The malware will intercept the host response message and modify it to a larger amount therefore the ATM will dispense far more money than what is debited from the account. A variation of the attack, is where the malware intercepts the request, and returns an authorization message such that the transaction host is unaware of the request.

- **Ransomware Attacks**

A serious malware called “WannaCry” encrypts the files on end-points that are running Microsoft operating system software, rendering them inaccessible. The files are only decrypted upon payment of a sum of money known as ransom. This malware attempts to infect other end-points on the same network. The malware does not specifically target Banking and Retail systems or their functionalities but ATMs like any other Windows based system are also at risk of this attack. There have been unconfirmed media reports that some ATMs in India have experienced this attack.

Prevention of infection via phishing emails by implementation of technical and organizational measures,

Segment and secure local area Network(LAN)/ virtual LAN(VLAN) with intrusion detection and prevention mechanisms to avoid infection and distribution of malware via the network,

- **ATM Jackpotting Attack**

The term ATM Jackpotting comes from the term Jackpot. In this type of attack, cyber-criminals get huge sums of money from the ATM at once. Cyber-criminals use two methods to perform this attack:

ATM INCIDENT MANAGEMENT POLICY AND PROCEDURES

The Bank has developed, communicated and implemented formal systems and procedures for detecting and reporting incidents relating to exceptional situations in day-to-day administration of IT and information security related areas. The Bank ensures that the incidents are reported in time to the appropriate authorities and corrective actions are taken immediately to provide the IT Service to Users as quickly as possible and to avoid the recurrence of such events in future

19. Definitions

"ATM" Automated Teller Machine is a computerized machine that provides the customers of banks the facility of accessing their accounts for dispensing cash and to carry out other financial transactions without the need of actually visiting a bank branch.

"Incident" is a term related to exceptional situations or any event which is not a part of the standard operation of a service and which causes or may cause an interruption to or a reduction in the quality of service or a situation that warrants intervention of senior management. An incident is detected in day to day operations and management of the IT function. This may be result of unusual circumstances as well as the violations of existing policies and procedures of the bank. An incident may relate to any of the following:

- ✓ Suspected hacking attempts
- ✓ Successful hacking attempts
- ✓ Loss of information due to unknown reasons
- ✓ Hardware resources and components lost / stolen
- ✓ Virus incidents regarding Internet and others
- ✓ Threat to Physical Safety of human beings.
- ✓ Attacks originating from the bank's and ATM network

✓ Threats, harassment, and other criminal offences involving individual user accounts.

✓ Compromise of individual user accounts on multi-user systems.

✓ Forgery and misrepresentation, and other security-related violations of local rules and regulations.

✓ Compromise of Desktop Systems.

✓ Events shall be classified as Critical, Key and Significant as detailed below

• **LEVEL**	• **Definition**
• Critical	• Any problem due to which 200 or more users cannot access the Business, Networking and environmental infrastructure system
• Key	• Any problem due to which 10 to 200 users cannot access the Business, Networking and environmental infrastructure system
• Significant	• Any problem due to which 1 to 10 users cannot access the Business infrastructure system

✓

20. **"INCIDENT RESPONSE**" set of actions taken to protect and restore the normal operating condition of computers and the information stored in them when an adverse event or incident occurs; involves contingency planning and contingency response.

21. **"INCIDENT HANDLING**" Same as Incident Response.

22. **"INTRUSION**" any intentional event where an intruder gains access that compromises the confidentiality, integrity, or availability of computers, networks, or the data residing on them

23. **"CHAIN OF CUSTODY"** verifiable documentation that indicates the sequence of individuals that have handled a piece of evidence and the sequence of locations where that evidence has been stored, including dates and times. For a proven chain of custody to occur, the evidence is accounted for at all times.

24. **"CONSTITUENCY"** Implicit in the purpose of a Computer Security Incident Response Team is the existence of a constituency. It is the group of users, sites, networks or organizations served by the team. The team must be recognized by its constituency in order to be effective.

25. **Responsibilities**

- ✓ Provide a (secure) channel for receiving reports about suspected incidents.
- ✓ Provide assistance to members of its constituency in handling these incidents.
- ✓ Disseminate incident-related information to its constituency and to other involved parties.

ROLE	RESPONSIBILITIES
Implementation	All IT users are expected to know whom to report the incident. The respective department personnel are responsible for their assigned IT domain.
Monitoring & Supervision	Security/System/Database and Network Administrators
Escalation	Assistant General Manager-IT /Deputy General Manager – IT / General Manager, IT

26. Procedures

✓ Functions of IT Department with respect to Incident management

✓ The System administrators shall handle the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management

✓ Incident Triage

✓ Investigating whether indeed an incident occurred.

✓ Determining the extent of the incident.

✓ Incident Coordination

✓ Determining the initial cause of the incident (vulnerability exploited).

- ✓ Facilitating contact with other similar sites who have reported the incident (if applicable).
- ✓ Facilitating contact with appropriate law enforcement officials, if necessary.
- ✓ Making reports.
- ✓ Composing announcements to users, if applicable.
- ✓ Incident Resolution Removing the vulnerability.
- ✓ Securing the system from the effects of the incident.
- ✓ Evaluating whether certain actions are likely to reap results in proportion to their cost and risk, in particular those actions aimed at an eventual prosecution or disciplinary action: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, etc. Collecting evidence where criminal prosecution, or Disciplinary action, if contemplated.

27. Data Collection & Analysis

- ✓ In addition, IT department will collect statistics concerning incidents which occur within or involve the bank's information resources, and will notify the relevant parties proactively as necessary to assist it in protecting against known attacks.
- ✓ The incidents noted are analyzed by the quality function on a semiannual basis to identify trends, if any. A database containing following information for each incident noted is prepared for future use:

28. Type of Incident

- ✓ Impact Analysis on the affected IT assets or business process
- ✓ Ways of detecting the incident

✓ Ways of resolution of incident

✓ Down time requirements

✓ Contact details for reporting and resolution

✓ Information Services: List of departmental security contacts, administrative and technical.

✓ These lists will be available to all users inside the bank and general public, via commonly available channels such as Intranet/World Wide Web.

- **Auditing Services:**

✓ System Administrator should arrange for Central file integrity checking service for various servers and for any other platforms capable of running file integrity checkers like “tripwire”.

- **Archiving Services**

✓ Records of previous security incidents handled will be kept. While the records will remain confidential, periodic statistical reports will be made available to the management.

✓

29. Incident Handling & Management

i. Constituency

✓ An IT Department's constituency can be determined in any of several ways. For example it could be a company's employees or its paid subscribers, or it could be defined in terms of a technological focus, such as the users of a particular operating system.

✓ The definition of the constituency should create a perimeter around the group to whom the team will provide service. The policy section of the document (see below) should explain how requests from outside this perimeter will be handled.

ii. Detection and initial reporting:

✓ An incident may be detected by anybody in the bank. The concerned personnel should immediately bring it to the notice of the person designated by IT department. The person so designated should escalate the issue as per escalation guidelines. The initial reporting covers following:

✓ Time of the incident

✓ Nature of the incident

✓ Probable cause of the incident

✓ Effect of the incident

✓ Mode of resolution of the incident

✓ Activity log in case the incident involves desktop / server / network operating systems or any of the applications.

iii. Documentation and formal reporting:

✓ A person designated by departmental head should maintain the central database of all such incidents. The person so designated, after analyzing the extent of exception and facts of the incident, should appraise the related IT department personnel. A detailed risk and impact analysis for the incident should be carried out by the IT team. (Refer to Annexure A, B and C for the formats of Incident management documentation).

✓ The IT department should ensure that all incidents are categorized based on the nature of each incident and are held in a database created for the purpose. The database should be able to provide information on demand and have the capability to perform analysis on the data contained within. The bank‘s employees encountering incidents would

thus be able to access the incident database and possibly find solutions if the incident had occurred before. Frequently asked questions should also be incorporated into the database to assist the user in finding solutions to incidents encountered.

iv. Monitoring:

✓ All the major incidents should be reviewed and monitored by the Security Administrator and discussed in the Technology Committee meeting every month. The magnitude and criticality of the incidents may prompt the System/Database/Network Administrators to discuss and take action on the incidents immediately instead of at fixed intervals.

v. Development of corrective action plan:

✓ The IT department, in consultation with affected System administrator or any other person it deems fit should prepare the corrective action plan for the incident. The action plan, though specific to each case, should typically cover the following:

✓ Facts and explanation / reasons for the incident

✓ Corrective action to be taken

✓ Estimated cost of implementing the corrective action

✓ Estimated time frame, start date and end date

✓ Personnel responsible for taking the action

✓ Information exchange with other Incident Handling teams

✓ The IT department can share information with other incident management teams and general public with prior permission from Executive Director.

✓ Annexure A –Incident Reporting Form

Department:	Date:

Name of the employee:	Department:
Facts of the incident:	
Signature:	

✓ Annexure B Reporting of the incident to Level 2

Department:	Date:
Incident reported by:	Incident occurred on:

Facts of the incident:	
Analysis of the incident by Head of Department and impact:	
Signature: Systems Administrator/ Operator incharge of the branch	Signature: Head

Annexure C Incident Management (Level 2)

Incident Number:	Incident Date:
Branch:	Date of reporting from the branch:
Facts of the incident:	
Risk and impact analysis:	

Discussed with Corporate Information Security Committee on:					
Corrective Action plan for incident management:					
#	Corrective Action	Responsibility	Start Date	Expected date of completion	Estimated cost