FRAUDS WITH PLASTIC MONEY : A CRITICAL ANALYSIS IN INDIAN SCENARIO

J. K. Das*

Pradipta Mukhopadhyay**

[*The Financial Institutions of India and the banking sector has undergone massive revolution over the past three decades in order to cater to the banking and financial needs for all in the most efficient yet simple manners. Digitalization has enabled users to access their accounts and carry on transactions without their physical presence. But this advancement has also given rise to various crimes which exploit the linchpins and limitations of these systems. Such cyber crimes are more dangerous in nature than regular ones, as it is often difficult to track the criminals, or authorities lack the knowledge to apprehend them. Cyber criminals are coming up with innovative ideas to dupe innocent victims of their hard earned money, one of the leading methods being Card frauds, both debit and credit. There are numerous weapons in the arsenal of criminals in this respect such as skimming, card trapping, stealing, pharming, key stroke logging, phishing scams, installing malware or viruses to name a few. This paper deals with the types of card frauds with special focus in debit and credit cards that are currently plaguing India, and how to combat them.*

Keywords: *Card fraud, Cyber Crime, Case Studies, Debit Card, Credit Card*]

Introduction

The modern thief can steal more with a computer than with a gun *(National Research Council, Computers at Risk).* Technological advancement and its omnipresence are supposed to be a boon to mankind but have started casting a darker spell instead. The modern era is witnessing close contact with computers and internet technologies that is extremely beneficial but at the same time possesses greater risk of violating peoples' rights and privacy. Cyber-attacks, malwares, identity theft, card frauds, phishing, spamming are few of the menacing cyber-security threats through which cyber criminals are operating to execute their malicious intents.

Cyber crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything is being run on computerized mechanisms, cyber crime has assumed rather sinister implications. The abuse of computers has thus given birth to a gamut

* Professor, Department of Commerce, University of Calcutta, E-mail: *jadabkdas@gmail.com*

** P & P Consultants, Business Management Consultant of Middle East and North Africa, Founder and Proprietor, E-mail: *pradipta1516@gmail.com*

of new age crimes that are addressed by the Information Technology Act, 2000. A simple yet sturdy definition of cyber crime would be "*unlawful acts wherein the computer is either a tool or a target or both*".

Today internet is the fastest infrastructure available to people where man is able to send and receive any form of information at any place instantaneously. At the same time, various modes of electronic payments such as debit/ATM cards, credit cards, the facilities of online banking/net banking etc. provides instantaneous credit services to avail various facilities in our daily lives *(Rohilla & Bansal, 2015)*. But with improved technology, cyber criminals too are becoming more sophisticated in targeting consumers as well as public and private organizations. Their prime target is however the various financial institutions, especially the banking sector, for its obvious access to unlimited money coupled with vulnerable customers. Banking frauds not only results in financial loss to the banking institutions but also undermine the customers' confidence regarding the security of their own hard earned money *(Saha and Rahman, 2018)*. Though the banking sector has long been creating new innovations to combat fraudsters in order to create a secure environment for financial transactions from holograms and the tamper-evident signature panel, card validation codes and EMV (Europay Mastercard and Visa) chip and PIN, Credit Verification Values, Address Verification Service, restricting the amount of withdrawal per transaction per day and the introduction of One Time Password (OTP) system for cash withdrawal from ATMs (Automated Teller Machines), still the number of incidents of frauds are at an increase with each passing day.

For more than past three decades, with the introduction of the first ever ATM in India in the year 1987 (in Mumbai), consumers across the country have become immensely dependent on the ATMs for conveniently meeting their banking and financial needs *(Jain, 2017)*. Similarly, recognizing the potential of credit cards, Indian banks issued them to persons with credit worthiness when ANZ Grindlays Bank launched the *classic cards* in 1989 followed by Citibank's *master and visa card* in 1990 *(Kathirvel, 2013)*. But this scenario has given fraudsters the opportunity to exploit such dependence and break into the larger money and banking sector system to steal funds from their customers.

Many researchers in their research works have identified this growing concern of breach of security regarding funds and have recommended a number of preventive measures to benefit the readers. With a great increase in credit cards, debit or ATM cards & E-transactions, frauds have been increasing excessively in recent years. Thus, a system based on cryptographic algorithm, which will find the exact user not only by the security PIN number for banks transaction but by asking security questions is highly advisable to reduce the probability of card fraud cases (*Meshram and Yenganti, 2013)*. Though there are many ways in which fraudsters execute an ATM card fraud, such as, Lost or stolen card, Account Takeover, Tampering or Altering Card Details, Fake card, Skimming etc., the technology of ATM is continuously developed and modernized yet, the fraudsters are always one step ahead in committing crime *(Saha and Rahman, 2018).* Therefore, banks must have an information security policy in place that tells the insiders how to tackle and combat any security breach. New technologies such as video surveillance, remote ATM management and both employee and customer education combined with common sense management practices aimed at deterring crime are providing an edge in the fight against fraud *(Jain, 2017).* In today's busy world, card transactions used for all the daily chores like paying bills, transferring money, buying cell phone charges, viewing transactions list, and many other services which the customers prefer doing without the need to be at a bank, and consequently banks also benefit from these services through customer retention and higher cash flow *(Barkhordari, 2018).* Therefore, it is crucial that the public receive clear communication on the measures taken by the different actors and on the steps that consumers can take to minimize risks. This communication should not make the public feel insecure. However, done in a suitable way, it should improve the perceived level of safety, stimulating consumers to feel safe in all circumstances *(Kosse, 2013).*

Increase in the number of banking frauds worldwide can be attributed to not only the increase in the number of cyber criminals, but also to lack of consumer education and awareness. Consumer education remains a pivotal part of the strategy to protect the cardholder's account information and to help banks and merchant businesses prevent losses. Keeping consumers informed about what they can do to protect themselves is a crucial preventive measure in the evolving global and regional fraud landscape. Being aware and staying vigilant about protecting their personal information can also greatly reduce risk of theft or fraud — an important and necessary step in today's digital world. While credit and debit cards have built in protections, the first line of defense really starts with the cardholder.

An Overview of Various Types of Card Frauds

Card fraud essentially involves thievery of information relating to the debit/credit cards of the consumers. The information stolen is further used to make conduct unauthorized online or offline transactions or ATM withdrawals by impersonating the aggrieved card holders. *Such stealing of ATM/debit cards can take place in one of the following ways (Jain, 2017):*

a) **Automated Teller Machines:** The Automated Teller Machines (ATMs) has become a preferred target for the fraudsters in the recent past as a clear rise is witnessed in the number of banking frauds related to ATM card transactions to rob customers of their savings.

b) **Shoulder Surfing:** Friendly onlookers in the ATM kiosks who offers help or peer over other card holder's shoulder during transaction, in all possibility wish to wrongfully collect such customer's PIN.

c) **Skimming:** Fraudsters with mal-intentions attach a *data skimming device* in the card reader slot of the ATM machines and once the debit cards are swiped, all information pertaining to the card are copied from the magnetic strips attached to the cards. Moreover cameras near the machine are hidden and placed in a way to get access to the PIN.

d) **Bulky Slot:** Bulky or misaligned ATM card slots indicates the presence of an additional card reader slot that has been placed on top of the actual slot for fulfillment of malicious intentions.

e) **Fake Keypad:** Like the false front, a fake keyboard too is installed on top of the actual keyboard of the machine by the fraudsters. Customers should be wary of spongy, loose or any other type of keypad which seems unnatural to them, and should not continue with their transactions.

f) **False Front:** False fronts are usually more difficult to perceive as it envelopes the entire machine and installed on top of it, as an outer shell, thus making it easier for the criminals to steal the customer's PIN details.

g) **Online Transaction:** The convenience of online shopping and making payment for the same via online transactions has led to loss of confidential information for many card holders.

h) **Pharming:** To extract valuable information, often customers are redirected to a fake website, an exact replica of the original one and when any payment transactions are made, all information gets stolen.

i) **Keystroke Logging:** Users very often downloads software, though unintentionally, that gives full access to the fraudster to track the card holder's key strokes thereby stealing passwords or online/net banking or credit card.

j) **Malware:** Malware stands for malicious software that targets the computer systems at ATMs or bank servers, damages them thereby allowing fraudsters to access confidential information.

k) **Phishing & Vishing:** Phishing involve identity theft through spam mails which seem to be from a genuine source, whereas Vishing is essentially the same through a mobile phone using messages or SMS. These trick the customer into revealing their password, PIN or account number.

l) **SIM Swipe Fraud:** In this case, the impostor contacts the customer's mobile operator with fake identity proof and gets a duplicate SIM card. The operator deactivates the original SIM and the thief generates one-time password (OTP) on the phone to conduct online transactions.

m) **Unsafe Apps:** Mobile applications other than those from genuine and official sources/stores can get access to all information in the mobile phone which can be later used for unauthorized transactions.

n) **Public Wi-Fi:** Any customer carrying out payment transactions on their smart phone using a public Wi-Fi has the risk of providing good hacking opportunities.

o) **Point-of-Sale Theft:** This technique involves taking the debit or credit card for transaction purpose by the salesperson in good faith but it indeed is an effective method of stealth of information to be used later for unauthorised transactions.

p) **Lost or Stolen Cards:** Lost or stolen cards mainly through postal intercepts are wrongly used to make unauthorized transactions since the information is compromised before reaching the owner.

On the other hand, credit card frauds can be broadly classified into the following categories (Kathirvel, 2013):

a) **Account Takeover:** Fraudsters having illegally impersonating any genuine person informs the bank of change in his official address. Thereafter wrongfully reporting their credit card as lost, requests for a new card to be mailed to their new address, thus gaining full access to the account.

b) **Identity Fraud**: It occurs when someone illegally obtains personal information and repeatedly uses it to open new account or to initiate transaction in the name of legitimate customer. Majority of identity thefts occur offline like stealing the wallets, intercepting the mail or rummaging through the trash.

c) **Postal Intercept**: Fraudsters intercepts cards or replacement cards sent via mail before it reaches the legitimate card holder.

d) **Counterfeit Card Fraud:** This is similar to skimming of Debit Cards. A counterfeit, cloned or skimmed card is one that has been printed, embossed or encoded without permission from the card company or one that has been validly issued and then altered or recorded. Most cases of counterfeit fraud involve skimming, a process where the genuine data on a cards' magnetic stripe is electronically copied on to another card, without the knowledge of the legitimate cardholder. Skimming can occur at retail outlets – particularly bars, restaurants and petrol stations.

e) **Lost or Stolen Cards:** Genuine cardholders lose their credit card or someone steals them for carrying out illegal transactions.

f) **Phishing:** Stealing of valuable information like the cardholders' account related information or other sensitive data via e-mail posing to be the cardholders' banker or seller where the cardholder has carried out recent transactions.

Cyber Fraud in India

Bank heists are a shortcut to riches and has evolved with time in India. A total of 1,012 incidents were reported across the country in 2016-17 (highest in the past financial year ended 2016-17, 2017-18 and 2018-19) The tally reduced marginally to 972 incidents in 2017-18 according to data collated by the Reserve Bank of India (RBI). The banking sector lost a total of Rs 168.74 crore to organised crime directed at ATMs in the past three years (*this includes figures for the first quarter of Financial Year 2019).*

However, in terms of the quantum of cash looted, there has been a slight improvement. From a high of Rs 65.3 crore in 2016-17, the amount of cash lost in ATM heists went down to Rs 44.49 in 2017-18. Between April and June 2018, 261 incidents were reported, entailing a loss of Rs 18.85 crore to banks. For the financial year ended March 2018, the maximum number of untoward incidents in banks and ATMs was reported in Bihar where the financial institutions lost Rs 3.35 crore from a total of 147 incidents. Security is also lax in Delhi and Haryana, where 53 and 49 ATMs were targeted respectively, resulting in the loot of cash amounting to Rs 2.25 crore and Rs 3.34 crore respectively.

In 2017, Mumbai city witnessed a 42% rise in cases related to credit and debit card fraud the detection of which however, went down by 28% during this period, as compared to the cases detected in 2016. In 2017, 606 cases related to debit and credit card fraud was registered across the city, as compared to 423 cases registered in 2016. As far as the crackdown of the cases are concerned, the police had succeeded to crack 54 cases in 2016, but could crack only 42 last year, taking the rate of detection from 12% in 2016, to roughly 7% in 2017.

Uttar Pradesh has consistently ranked among the riskiest state for lenders with 85 heists at ATMs, setting back banks by Rs 2.09 crore in 2017-18. West Bengal also witnessed over 100 such incidents in the same financial year.

With a lot of essential financial services shifting to the digital space, the number of frauds targeting online transactions has also increased. In 2017-18, a total of 911 frauds were committed using debit and credit cards where a sum total of Rs 65.26 crore went into the wrong hands.

The most number of card frauds were targeted at ICICI Bank customers in 2017-18. As many as 348 cases were reported, wherein Rs 7 crore was embezzled. State Bank of India customers were defrauded to the tune of Rs 10 crore, in 144 reported cases. However, the biggest fraud happened at City Union Bank, where Rs 32 crore was stolen in a single case.

India is witnessing a surge in digital payments thanks to Prime Minister Narendra Modi's 2016 decision to recall 86% of cash in circulation, and his government's aggressive push for a more cashless economy. The number of credit cards rose by a quarter to more than 38 million in the 12 months ending in May 2017, while the number of debit cards jumped 17% to over 925 million in the same period, according to RBI data. But many of the cards continue to come with magnetic strips which store all important customer data and are more vulnerable to cloning.

India was ranked among the top 5 countries with regard to credit card fraud, with more than one third of the people saying they had been scammed, according to the 2016 Global Consumer Fraud Report published by payments technology company ACI Worldwide.

Moreover, the Reserve Bank of India (RBI) has registered a total of 921 cases of fraud involving ATM/debit cards, credit cards and Internet banking, wherein the amount involved was Rs 1 lakh and above, during the financial year 2018-19 (up to September 30, 2018). During the financial year ended 2015-16, 2016-17, 2017-18, the number of such cases of fraud registered by the RBI stood at 1,191, 1,372 and 2,059 respectively. The capital of India, Delhi, reported 179 cases of ATM frauds in 2018-19, the second highest in the entire country as per Reserve Bank of India.

On 3rd August 2018, several people in Kolkata have reported ATM frauds in which 78 customers of some leading public and private sector banks have allegedly lost over Rs 20 lakh.

Again, on 19th October 2018, State Bank of India (SBI) blocked 6 lakh debit cards after a reported malware-related breach in a non-SBI ATM network. This was possibly India's largest financial data breach where nearly 32 lakh debit cards across 19 banks both public and private were compromised. As per the reports of the National Payments Corporation of India (NPCI), over 90 ATMs were impacted and at least 641 customers lost around Rs 1.3 crore in fraudulent transactions.

Maharashtra reported 233 cases of ATM fraud in 2018-19, the highest in the entire country as revealed by the Reserve Bank of India (RBI). The data showed that Delhi grabbed the second spot with 179 cases, followed by Tamil Nadu with 147 cases of ATM fraud. In Maharashtra, people lost Rs 4.8 crore to bank fraud, while in Delhi people lost Rs 2.9 crore. The country witnessed an increase in ATM fraud cases in general (up from 911 to 980). Assam, Arunachal Pradesh and Tripura were the only three states that didn't report a single incident. However, the money lost came down from Rs 65.3 crore in 2017-18 to Rs 21.4 crore in 2018-19.

Even as RBI and the banks are trying to stay one step ahead by introducing several security features, customers need to take the initiative to prevent being conned. Consumer education is a pivotal measure, at not only preventing but also apprehending such criminals who are intent on carrying out fraudulent activities. Vigilance is required by all the stakeholders to reduce and curb the growing menace that is- ATM Card fraud.

Few Case Studies

a) **In august** 2014, a Mumbai resident came face to face with illegal online transactions, when he received two alerts notifying him of transactions being made from his credit card in Netherlands and Australia worth Rs. 12,000/-. The aggrieved party immediately notified his bank of the same and blocked his card. The bank in turn advised him to get a new card in lieu of the old one. Despite repeated requests of resolving the issue first, the bank not only sent the aggrieved party the credit bill of the huge amount of money he "allegedly" spent, but also charged huge amount of interest on the same, despite there being foul play. (*The Economic Times, October 26, 2018*)

b) **Another Mumbai resident** faced an unusual situation in February of 2016 when she inserted her card in an ATM machine to withdraw money. Due to the nonperformance of the machine, she had to move on to the next ATM to withdraw a sum of Rs. 2500/-. But within a few minutes, she received an alert stating that Rs. 10000 has been withdrawn from her account. Despite contacting both the banks for video footage, the banks not only refused to share the same, but also denied remittance of the Rs. 10,000/- which was fraudulently taken away from her (*The Economic Times, October 26, 2018*).

In the year 2019, various cases of Card Fraud took place all over India, some of which are mentioned below

c) In Delhi, an archetypal case of shoulder surfing left many victims harassed when their cards were used to withdraw money from their banks and other fraudulent activities. The accused criminal targeted ATMs without any guards, having machines which were malfunctioning or freshly out of cash. Then on the pretext of helping the victim, he would learn the ATM pin by the method of shoulder surfing and later swap the actual card with a fake one. Thus armed with both the card and the pin, the accused used them to withdraw cash. When apprehended, cash over Rs. 30,000/-, two new smart phones and around 20 ATM cards were seized from the accused *(Business Standard, July 14, 2019).*

d) The police were able to apprehend two Turkish and two Bangladeshi nationals for allegedly hacking several State Bank of India ATMs across the country including Guwahati, Agartala, Delhi, Mumbai, Kolkata and stealing crores of rupees from innocent SBI customers. The accused used skimmer devices to clone the original ATM cards of the customers. The two Turkish nationals are not new to this crime, they already have 46 prior cases registered against them (*NDTV, November 19, 2019*).

e) As many as 30 salaried people in Kolkata were targeted in a case of what the police suspected to be of ATM skimming, where these victims lost their hard earned money to ATM transactions not carried out by them. The police suspected that the criminals must have got hold of old card data and have used them to cheat the victims (*Live Mint, December 03, 2019*).

f) Also, in a separate incident, two people of Romanian national were arrested in connection with stealing ATM card details using cameras and skimmers, thereby making clones of the original cards to launder money (*The Hindu, October 25, 2019*).

g) Ahmedabad based man was robbed of Rs. 2.61 Lakh from his credit card in an unauthorized international transaction when surprisingly he did not receive any SMS intimation or OTP confirmation for the same from his bank (*The Times of India, November 19, 2019*).

h) Cybercrooks made online transactions of 3,372 pounds (Rs. 3.3 lakh) in London by cloning the credit card of a Pune based software engineer. The probe further revealed that the credit card was used in four spots in London mostly for bed and breakfast purposes (*The Times of India, February 01, 2020*).

i) Punjab based man experienced a credit card fraud where in his credit card was illegitimately used by a Lahore based fraudster to do shopping worth Rs. 1.15 lakh. Judgment is still pending on the case (*The Times of India, February 21, 2020*).

A Primary Survey

For the purpose of procuring some authentic responses, 100 people (74% of male respondents and 26% female respondents) were interviewed via primary survey regarding their views and experiences on card fraud, residing at different parts of India, ranging from 18 years to above 60 years of age. Where 58% respondents prefer to deal with card transactions, 40% of them chose cash transactions as their preferred mode. Yet for the purpose of withdrawal of money, 79% of the respondents withdraw their money with the help ATM card transactions. In today's busy world, people more often tend to simplify their work by using ATMs as a mode of withdrawal and deposition of money, which in turn acts as a simpler method of completing their daily chores. Irrespective of long queues, link failure, occasional non availability of cash, ATMs are still the preferred choice for 90% of the respondents due to its round the clock accessibility. Moreover, 70% of the respondents opt for their cards for any kind of payment transactions. 30% of the respondents have had a bad experience associated with card frauds, from getting fraud calls to extract their personal information via phone or e-mails to suffering monetary loss due to hacking.

No matter how advanced security measures are adopted by the banking sector, fraudsters seem to be always one step ahead of them. And the most important set back is that people are not well aware of the precautionary measures that need to be taken from their end coupled with lack of legal knowledge. 90% of the respondents believe that the Indian legal framework is not adequate or strict enough to deal with such fraud cases and among the respondents 55% are not even aware of their rights as the aggrieved party as well as remedial measures that could be opted for incase of any fraud cases. Moreover, lack of cyber awareness leads to 80% of frauds *(News 18, 2019)* and thus increasing awareness is the first and the most important measure to combat this growing security threat. Even 78% of the respondents themselves believe that awareness is the only way to fight the growing threat that is cyber crimes. Thus, with the growing dependence on today's world on computers and digital mediums it is the responsibility of every stakeholder to ensure safety for themselves and others in this new online digitalized forum from the sinister intent of the cyber criminals.

Conclusions and Recommendations

Everyday, cyber criminals are coming up with innovative ideas to dupe innocent victims of their hard earned money, one of the leading methods being ATM or Card frauds. Such cyber crimes are more dangerous in nature than regular ones, as it is often difficult to track the criminals, or authorities lack the knowledge to apprehend them. There are numerous weapons in the arsenal of criminals in this respect such as skimming, card trapping, shoulder surfing, pharming, key stroke logging, phising to name a few. And to combat this evil, the card holders need to be more responsible and vigilant regarding maintaining their card's secrecy. For further safety of credit card users, such transactions are provided with a buffer time period of one month before the amount is deducted from the account holder's account within which time, if the card's information has been compromised with, it can be investigated upon. Consumer education is another key element in combating ATM card fraud incidents as it helps lessen the gullibility and vulnerability on their part, which often turns out to be the Achilles heel of the Banking system. An aware customer is the best first line of defense the banking sector can hope to have.

Public awareness is pivotal for putting a stop to the rampant ongoing cyber frauds. Next comes the responsibility of the respective institutions of the banking sector that is the main target of fraudsters, to ensure that preventive measures are taken up and to also ensure high end security for its customers**.** As technology has upgraded itself to greater heights in providing all possible services to the public, it has also reached greater heights in jeopardizing the safety and security of the same. Continuously our privacy is being compromised and our personal information is absolutely laid bare to the cyber criminals, having malicious intents.

Some basic, preventive steps that can help people avoid falling prey to credit or debit card fraud are as follows

Debit Card Fraud Safeguards

While using Debit or ATM cards, some points to be kept in mind by the customers are as follows:

- **Machine Safety:** Machines that have unusual signage or commands, or which appears to have been tampered with or altered, or if its front structure looks crooked or loose, such machines should be avoided as they might have skimming devices installed to duplicate and steal card data
- **Keypad Usage:** It is of utmost importance that while entering the PIN, it must be covered with hand to escape the gaze of shoulder surfers or from any nearby hidden cameras if attached.

ATM Kiosk: It is prudent to use the debit cards in respective bank ATMs, particularly those attached to a bank branch and those with the presence of security guards. Also, taking over friendly strangers help in an ATM should be strictly avoided to protect oneself from being duped.

Online Preventive Measures

- **Safe Website:** It is advisable to visit only trusted and recognized sites for indulging in online shopping. The site's legitimacy should be confirmed before using it and the user should also check for Secure Sockets Layer (SSL)-certification, which is indicated by the lock symbol next to the browser's URL box. Also it is better to use sites with 'https' protocol instead of 'http', where 's' stands for 'secure'. Additionally, it is ill-advised to click on the option that asks for saving your card details on any site.

• **Log out:** Logging out of the social media accounts or other online accounts helps ensure data security.

• **Password:** Passwords should be changed frequently to reduce the probability of identity theft.

• **Anti-virus Software:** On an individual level, each person should ensure their own safety by ensuring their device's safety by way of installing anti-virus software on their computers and smart phones to safeguard their transactions.

• **Card Verification Value:** For online transactions often the CVV is required to be entered which is the only point of verification. Therefore it is advisable to use a virtual keyboard to avoid keystroke logging thereby securing valuable information.

• **Security Alerts:** Alerts and notification from bank act as an early warning sign in case of unusual or unsanctioned online card transaction or ATM withdrawals the moment they take place.

• **Public Wi-Fi:** People should avoid using unsecured or public Wi-Fi networks since they are easy targets for extraction of personal information.

Offline Preventive Measures

Some additional precautionary measures on top of the ones mentioned above are:

• **Card Details:** It is of utmost importance that the card holders under no circumstances should share any information relating to their cards, be it the PIN, CVV or password to anyone. Extra care should be taken to avoid responding to any such e-mails or SMSs that ask for crucial personal or card-related details since no bank or credit card firm is authorised to seek any such information from customers via mail or over the phone.

• **Bank Statements:** Card holders should be vigilant enough to identify any unauthorized transaction by way of keeping a regular tab on their bank statements.

• **Merchants & POS:** It should be ensured at all times that while making payments the card should not leave the possession of the card holder as card information can easily be copied and stolen in such cases. Moreover it is advisable to opt for chip-enabled card readers for completing payment since this helps bring down the risk of fraudulent card activity significantly.

Call for Immediate Action

• In case of card theft or identity theft or a fraudulent offline/online transaction, the aggrieved parties are required to report such loss or wrongdoing immediately to the card provider or the bank and immediately have the card blocked. Along with an official email or a letter to the concerned authority, it is prudent to lodge an FIR with the police as soon as the customer is able.

• In case the bank is fails to respond within seven days time, the aggrieved parties are required to approach the nodal officer. If the bank fails to respond within 30 days, then the customers should contact the banking ombudsman appointed by RBI. If this too fails, the aggrieved party should approach the court of law for redressal.

Credit Card Fraud Safeguards

There are different key measures, which are used for detecting and preventing credit card frauds. Some of them are as follows:

a) **Credit Verification Values (CVV):** This technique verifies the last 3-4 digit number embossed on the card, its advantage being that physical possession of card is required for gaining access to the said information

b) **3D-Secure:** This technology works by authenticating the cardholder using previously recognized password. The fraudsters need the legitimate password to take control of the card, but often such passwords can be hacked, rendering their protection ineffective.

c) **AVS or Address Verification Service:** In this process, the customer's billing address and ZIP code are matched with the bank records at all times

d) **Relocation:** Relocation process tries to verify the customer's geographic location which is often based on their IP addresses. Its advantage lies in flagging or blocking orders which originate from high-risk areas. However, it cannot be applicable on 'IP proxies' and satellite.

e) **Chip and PIN:** The smart cards use an encrypted EMV chip which stores all information along with a PIN, which is used to provide proof of ownership of the card.

f) **Experts:** A team of experts who carry on and supervise various activities relating to the transactions is required to ensure that the technology used for the same has proper protection and is well managed at all times

g) **Biometric:** This is one of the recent and sophisticated additions in the fight against frauds. Unique characteristic of the customer like fingerprints, signature, iris or retina, voice or other similar biological components are recorded and stored to be read by computers, which is then compared to the already stored information of the cardholders. Despite its greater scope and sophistication, customers are often reluctant to accept this due to greater expenses.

Industry Collaboration: This allows any industry as a whole to collaborate as a united team for the purpose of safeguarding the interests thereby combating against any frauds.

General Preventive Measures – Debit & Credit Card

- The card (both debit and credit) should be kept within sight at all times
- The customer should always register their mobile number as well as their authentic mailing address (e-mail) with the bank and subscribe for alerts for any transactions. The bank should be contacted immediately in case of any suspicious activity, so as to get the card blocked
- The ATM should be checked properly so as not to carry any transaction on a faulty or rigged machine

• The CVV number can be memorized and then scratched out from the card

• Most importantly, customer awareness regarding the safety of their personal possessions (cards, money, personal information) is of utmost important in the fight against fraudulent activities.

References

- 4 Foreigners Hack ATMs, Dupe SBI Customers Of Crores, Arrested: Police (2019, November 19). *NDTV.* Retrieved from https://www.ndtv.com/india-news/atm-fraud-in-assam-4-foreigners-hack-atms-dupe-sbi-customers-of-crores-arrested-near-kolkata-police-2135234
- 6-12 hour gap between ATM withdrawals? (2019, August 27). *The Times of India.* Retrieved from https://timesofindia.indiatimes.com/business/india-business/6-12-hour-gap-between-atm-withdrawals/articleshow/70850574.cms
- 30 ATM card holders from a Kolkata locality complaint of fraudulent withdrawals (2019, December 03). *Live Mint.* Retrieved from https://www.livemint.com/news/india/30-atm-card-holders-from-a-kolkata-locality-complaint-of-fraudulent-withdrawals-11575345425275.html
- 42% rise in card fraud cases in Mumbai, but detection dips (2018, February 17) *hindustan times.* Retrieved from https://www.hindustantimes.com/mumbai-news/42-rise-in-card-fraud-cases-in-mumbai-but-detection-dips/story-Ff2B4UgggdNtbiVrTdRNtL.html
- Ahmedabad man swindled of Rs 2.6 lakh in international credit card fraud (2019, November 19). *The Times of India.* Retrieved from

  https://timesofindia.indiatimes.com/city/ahmedabad/man-swindled-of-rs-2-6-lakh-in-international-credit-card-fraud/articleshow/72046598.cms
- ATM Fraud. *NDTV.* Retrieved from

  https://www.ndtv.com/topic/atm-fraud
- ATM Skimming: Read this to save yourself from the new ATM fraud (2018, August 03). *The Economic Times.* Retrieved from

  https://economictimes.indiatimes.com/industry/banking/finance/banking/atm-skimming-read-this-to-save-yourself-from-the-new-atm-fraud/articleshow/65255952.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- Barkhordari, Mohammad Hossein (2018). Self-Payment Fraud Detection on Automated Teller Machine. *Current Trends in Computer Sciences & Applications, 1*(1), 3-11.
- Credit, debit card frauds and how you can avoid them (2018, October 26). *The Economic Times.* Retrieved from

  https://economictimes.indiatimes.com/wealth/spend/how-to-avoid-card-fraud/articleshow/55127030.cms?from=mdr
- Credit card fraud on the rise in India: how to protect yourself (2018, July 23) *national herald.* Retreived from

  https://www.nationalheraldindia.com/india/credit-card-fraud-on-the-rise-in-india-how-to-protect-yourself
- Dubey, Rajkumar. (2004). India: Cyber Crimes "an unlawful act where in the computer is either a tool or a target or both"– In Indian Legal Perspective. Retrieved from

  http://www.mondaq.com/india/x/28603/technology/Cyber+Crimes+an

+unlawful+act+where+in+the+computer+is+either+a+tool+or+a+target+or+both

- Delhi lost Rs 2.9 crore to ATM frauds in a year (2019, July 22). *The times of India.* Retrieved from

  http://timesofindia.indiatimes.com/articleshow/70321714.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

- Jain, Shubhra. (2017). ATM Frauds – Detection & Prevention. *International Journal of Advances in Electronics and Computer Science, 4*(10), 82-89.
- Kosse, Anneke. (2013). The Safety of Cash and Debit Cards: A Study on the Perception and Behavior of Dutch Consumers. *International Journal of Central Banking, 9*(4), 77-98.
- Kaur, Navneet. (2018). Introduction of cyber crime and its type. *International Research Journal of Computer Science, 5*(08), 435-439.

  https://www.academia.edu/37288317/INTRODUCTION_OF_CYBER_CRIME_AND_ITS_TYPE

- Kathirvel, K. (2013). Credit card frauds and measures to detect and prevent them. *International Journal of Marketing, Financial Services & Management Research,* .2(3), 172-179.
- Lack of Cyber Awareness Among People Leads to 80% of Frauds: Experts (2019, October 14). *News 18.* Retrieved from https://www.news18.com/news/india/lack-of-cyber-awareness-among-people-leads-to-80-of-frauds-experts-2344787.html
- Ludhiana: Man uses else's credit card to do shopping worth Rs. 1 Lakh (2020, February 21). *The Times of India.* Retrieved from https://timesofindia.indiatimes.com/city/ludhiana/man-uses-elses-credit-card-to-do-shopping-worth-rs-1l/articleshow/74233690.cms
- Man arrested for ATM fraud from southeast Delhi's Okhla Industrial Area (2019, July 14). *Business Standard.* Retrieved from

  https://www.business-standard.com/article/pti-stories/man-arrested-for-atm-fraud-from-southeast-delhi-s-okhla-industrial-area-119071400467_1.html

- Meshram, Pratiksha L. & Yenganti, Tarun. (2013). Credit and ATM Card Fraud Prevention Using Multiple Cryptographic Algorithm. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(8), 1300-1305.
- Maharashtra tops in ATM frauds, Delhi, Tamil Nadu, Karnataka follow. *Business Standard.* Retrieved from

  https://www.business-standard.com/article/finance/maharashtra-tops-in-atm-frauds-delhi-tamil-nadu-karnataka-follow-119072200187_1.html

- National financial Switch. Retrieved from

  https://en.wikipedia.org/wiki/National_Financial_Switch

- Net banking and card frauds up 50%, Delhi is ATM con capital (2019, December 11). *The Times of India.* Retrieved from

  https://timesofindia.indiatimes.com/india/net-banking-and-card-frauds-up-50-delhi-is-atm-con-capital/articleshow/72465160.cms

- Payments Management: Eight Different Types of Credit and Debit Card fraud (2014, November 03). *CFO Innovation.* Retrieved from

  https://www.cfoinnovation.com/risk-management/payments-management-eight-different-types-credit-and-debit-card-fraud

- Pune techie loses Rs 3.3 lakh in credit card cloning fraud (2020, February 1). *The Times of India.* Retrieved from

  https://timesofindia.indiatimes.com/city/pune/techie-loses-rs-3-3-lakh-in-credit-card-cloning-fraud/articleshow/73817645.cms

- Rohilla, Anju & Bansal, Ipshita. (2015). Credit Card Frauds: An Indian Perspective. *Advances in Economics and Business Management (AEBM)* 2(6), 591-597.

- Sankhwar, Shweta & Pandey, Dhirendra. (2016). A Safeguard Against ATM Fraud. *IEEE 6th International Conference on Advanced Computing.* Retrieved from

  https://www.academia.edu/29611551/A_SAFEGUARD_AGAINST_ATM_FRAUD

- Saha, Anuva Rani & Rahman, Md. Mijanur. (2018). Automated Teller Machine Card Fraud of Financial Organizations in Bangladesh. *Journal of Computer Science Applications and Information Technology, 3*(6), 1-6.

- The 8 Different Types of Card Fraud (2014, October 28). *Mastercard.* Retrieved from https://newsroom.mastercard.com/asia-pacific/2014/10/28/8-different-types-card-fraud/

- The growing cyber crime market. Retrieved from https://race.reva.edu.in/the-growing-cyber-crime-market/

- Two Romanians on a mission to clone bank cards arrested (2019, October 25). *The Hindu*. Retrieved from

  https://www.thehindu.com/news/cities/Hyderabad/two-romanians-on-a-mission-to-clone-bank-cards-arrested/article29790972.ece

- You may not be able to use ATM twice a day if banks have their way (2019, August 27). *The Economic Times.* Retrieved from

  https://economictimes.indiatimes.com/industry/banking/finance/banking/atm-frauds-could-lead-to-6-12-hour-gap-between-withdrawals/articleshow/70852655.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst