1 Senior Citizen Priority Fraud Response System (SCPFRS) "Click Karo, Complain Karo, Calm Raho"

Dr. Narayanan Anantharaman*
Vice President at YES Bank.

*Corresponding Author: narayanan_siws@yahoo.com
DOI: 10.62823/MGM/2026/9789349468795/01

Abstract

Senior citizens are increasingly becoming victims of cyber fraud due to various factors such as limited digital literacy, emotional vulnerability, and the accumulation of lifetime savings. Fraudsters exploit fear, impersonation tactics, and psychological manipulation to coerce senior citizens (victims) into sharing confidential banking information. In many cases, due to a lack of support, fraud is reported late, resulting in significant financial losses.This model proposes the Senior Citizen Priority Fraud Reporting System (SCPFRS) — a one-click emergency reporting mechanism integrated within the bank's mobile application. The system enables immediate account freezing, parallel alert generation to the Fraud Risk Management (FRM) team, and automated complaint registration with the cybercrime portal during the 'Golden Hour'.

Keywords: Fraud Risk Management, Golden Hour, Scams, Phishing, Fake Investment.

Introduction

India has witnessed a sharp increase in cyber fraud targeting senior citizens. According to industry surveys, there has been a significant rise in fraud cases involving identity theft, digital arrest scams, phishing, and fake investment schemes. Losses due to cyber fraud have reached alarming levels in recent years.Many senior citizens prefer traditional banking methods and may struggle to react quickly during high-pressure, potentially fraudulent situations. Fraudsters exploit this delay to execute multiple transactions before the incident is reported.

Case Illustration

A senior citizen residing alone received a video call from a fraudster, impersonating a police official. The senior citizen was threatened with a fabricated arrest warrant and instructed to share banking details. Under emotional distress, the victim disclosed the information, such as card details. Within a few seconds, the hacker performed a series of transactions before assistance could be sought. The senior citizen

reported the First Information Report (FIR) through a conventional channel much later after the incident. The Golden Hour had already elapsed, reducing recovery probability.

Problem Statement

- Senior citizens need assistance in quickly reporting cyber fraud incidents.
- The current traditional method of reporting is an afterthought once the incident is past.
- Cyber fraud awareness is lacking among senior citizens.
- The lack of an integrated model between the customer, the bank, and the regulators.

Proposed SCPFRS Mechanism

The SCPFRS introduces a dedicated 'Senior Citizen Priority Fraud Reporting' button within the bank's mobile application.

- One-click emergency trigger within the mobile banking app.
- Instant verification of the registered mobile number.
- Immediate temporary freeze of linked accounts in the Core Banking System (CBS).
- Automatic Priority-1 alert to Fraud Risk Management (FRM) team.
- Parallel automated complaint generation on the Cyber Crime Portal.
- Transaction monitoring and tracing by the FRM team.
- Controlled account reactivation post verification and customer consent.

Expected Outcomes & KPIs

- Reduction in complaint reporting turnaround time from hours to under 1 minute.
- Significant reduction in further unauthorized transactions post the first instance of the incident.
- Improved probability of fund recovery within Golden Hour (i.e., within 60 minutes of the first occurrence of the incident).
- Increase in customer (senior citizen) confidence and satisfaction by 70%.
- Strengthened collaboration between the bank and cybercrime authorities.

Long-Term Impact

The bank can implement the SCPFRS model for other user segments, such as homemakers, minor account holders, and differently abled users. It enhances digital trust, reduces systemic fraud exposure, and positions the bank as a socially responsible institution.

Case Study

Background & Context

Senior citizens in India are facing a tough time in getting adaptable to the latest technology. The modern way of banking is going digital and medium such as mobile banking, internet banking etc. is playing a major role. The adopting of the new technology

and gadgets are still disjointed with the senior citizen's daily usage. Many of them prefer the traditional way of banking i.e., visiting the branch for performing the paperwork and transaction rather opting for the digital banking. Hackers are taking advantage of such gaps, and they see the senior citizen as an easy prey in the cyber space for earning money through fraud. They use the weapon such as emotional intelligence and knowledge gaps among senior citizens. In few scenarios where the senior citizens are alone, they are more prone to such consequences. Based on the report shared by Safter Internet India there is 86% increase in the senior citizen getting victimized between 2020 and 2022. Further as the digitization is taking its gear, the use of mobile phones is increasing ad as per the statistics 61% who are in 60 to 69 and 45% above 70 years use mobile. On the other side of the story the as per Indian Cyber Crime Coordination Center (I4C) the losses due to cyber frauds was around Rs. 11,000 Cr in past years.

- **Brief on setting: geography, stakeholders, institutional environment**

In India we see day in and out with many frauds that are targeted to the senior citizens and further trapping them into a digital arrest kind of situation and in parallel their money is asked to be transferred into parts. Though government has initiated ways to spread awareness through various channels and even banking sectors are supported to share the flyers, but the senior citizens need additional support to respond to the situation as quicker as possible. The main reason for senior citizen getting targeted as per Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011) is because their thinking capability and slow pace in reacting to sudden situation weakens and thus they fall a prey in such situation.

- **Detail case which is presented.**

A case where a senior citizen Mr. ABC was staying alone in Mumbai and the daughter of the women was staying in another part of the country with her family. He received a video call from a fraudster through WhatsApp confirming to be a senior police inspector. He further conveyed to Ms. ABC to isolate himself in a room and follow the instruction. The fraudster further explained that there is an arrest warrant against Mr. ABC on having falsified account in the bank and this was used for money laundering. With the increase in stress Mr. ABC was not able to react on and waiting for further instruction. The Fraudster asked him to share the bank details and threatened that in case not shared then an arrest warrant will be issued. The fraudster disconnected the call and when the victim tried reach back the number, it was going into unreachable mode. In the very next moment, the fraud executed the transactions, and the amount was getting washed and multiple transactions happened to various fake account that was set by the fraudster. Finally, when the entire sequence was completed, the fraudster disconnected the call, and the number wasn't reachable. Due the shock of losing money the victim was helpless and was simply following the instruction.

- **Need for action/intervention**

As per the article in Times of India [3], it true that calling 1930 within the Golden Hour can help in saving your money and can control the damage. but in our case since there was no one to help the senior citizen, same would be executed with assistance. By

then the Golden Hour would have passed. Rather by the way of such mechanism the freezing of the account could be done much earlier.

Challenge / Problem Statement

In the present scenario the senior citizen is usually baffled when the get through such scenarios and once the entire digital arrest gets completed, the afterthought is to book a complaint either to the nearest police station or dial 1930, by this time the entire money is routed to reach the fraudster.

- **Specific issue and its implications**

During the scenario as defined above the time during which the call reaches the cyber cell and delayed and hence mostly, we see the “golden hour” is lost. Even in the above case the timeline for reporting the case is delayed and hence the probability of recovery the money or further damage on multiple transaction happing could be avoided. Since the victim has shared the bank details, even the system could be tricked on the transactions as it would seems that the customer is making the genuine money transfer.

Strategic Approach & Interventions

With the integration of the mechanism suggested, both the cyber cell and the bank can integrate help in reducing the amount that is being otherwise would lead to a huge amount. The mechanism can act as a double edge sword. As we spoke in the earlier section that a click would ultimately block the account where the victim can at least be sure that his further money might not be lost by this mechanism.

The mechanism and flow:

- Senior citizen would receive a call from fraudster asking for money and in case the bank details.
- In fear the Senior citizen would disclose the bank details to the fraudster
- Once the bank details are shared the phone gets disconnect and there is no way to reach the fraudster on the number from where the call was received
- The senior citizen could immediately hit on the “senior citizen priority fraud reporting button.
- The request will flow to the bank environment especially to the CBS system where the mobile number will be checked against the bank records and if found the corresponding account will be blocked.
- In parallel there a Priority 1 request will be raised in the Bank’s Fraud risk management system
  - The FRM team then start investigating the incident.
  - FRM team would check if there were any unauthorized transaction happened or if there is any initiation of unauthorized transaction with bulk amount is requested then such transaction would be blocked.
  - Or the case where the transaction has already been initiated and the amount is in the process of getting transferred or already transferred then the tracing of the same takes place.

  - Finally, the FRM would provide the detailed investigation report and if necessary, shall share it with cyber cell.
- In parallel there would be another request send to cybercrime portal to raise a compliant on the incident
  - The cyber cell team would there by start investigation the incident.
  - In association with bank's FRM team the cyber cell would be able to get the data on the transaction and the routing mechanism
  - Post the investigation, the cyber cell could try to identify the fraudsters and try to recover money based on the path through which the money was transferred or if the initiation of money has happened.
- Once the entire investigation is completed, the account holder will be initiated by the call or SMS or email or all to help in sharing their consent to reactivate the account.
- The account holder could either visit to the branch or shall book an appointment where the bank personnel could do a home visit and enable the account.
- The Bank shall help the senior citizen to get the app re-installed in the system and then try to change the credentials of bank's app in the mobile

Image 1: Senior Citizen Priority Fraud Response System

Source**:** Author-generated conceptual illustration created using AI-based design tools.

Steps taken, tools used, timeline, collaboration.

The implementation of this technique could be a simple feature to be added in the existing mobile banking app. Which could directly speak to the Core banking system and the cybercrime portal in parallel.

Innovations or deviations from standard procedures

As per the system there is no deviation in the standard procedures, it is an enhancement to the existing system.

Outcome & Impact

With the minimal efforts and assistance, the senior citizen could quickly react on the situation and stop further loss of money during the digital arrest or any such unforeseen situation. Even though the fraudster may get the OTP and other bank details with him, an account blocking can no longer allow even the hacker to transfer the money and thus the loss of money could be significantly reduced. As there is a probability of reporting on time the senior citizen would get confidence that the money loss could be reduced in such case which will improve the overall customer satisfaction for the bank.

- **Measurable results (data, KPIs, beneficiary feedback)**

  The impact on the KPIs:

- **Turnaround time reduction to report a complaint**: With a click the immediate action would be taken within no time, the actual time of reporting could be automated and reduced [1]. And the necessary action from the bank and the cyber cell be done within the first golden hours.
- **Loss reduction in further fraud transaction**: The fraudster in many cases would try to perform a sequence of transaction, a quick reporting and blocking of account would reduce the overall damage with no further transaction allowed via the account of the victim.
- **Increase in customer satisfaction**: As the damage could be controlled if not fully nullified, the customer would be happy that bank and cybercrime have tried to reduce the damage which is otherwise would have NIL their bank account.
- **Increase in the probability of recovering stolen amount**: There might be possible that the fraudsters might have stolen some amount before the blocking, but if the compliant is done within the golden hours of the fraud, there is increase in the probability that the amount could be recovered.

Long-term implication on business/process

- As we suggest having this implemented for the senior citizens at present.
- Same could be extended to the women's (homemakers) to reduce the over crime especially fraudsters targeting to steal money.

Learnings & Replicability

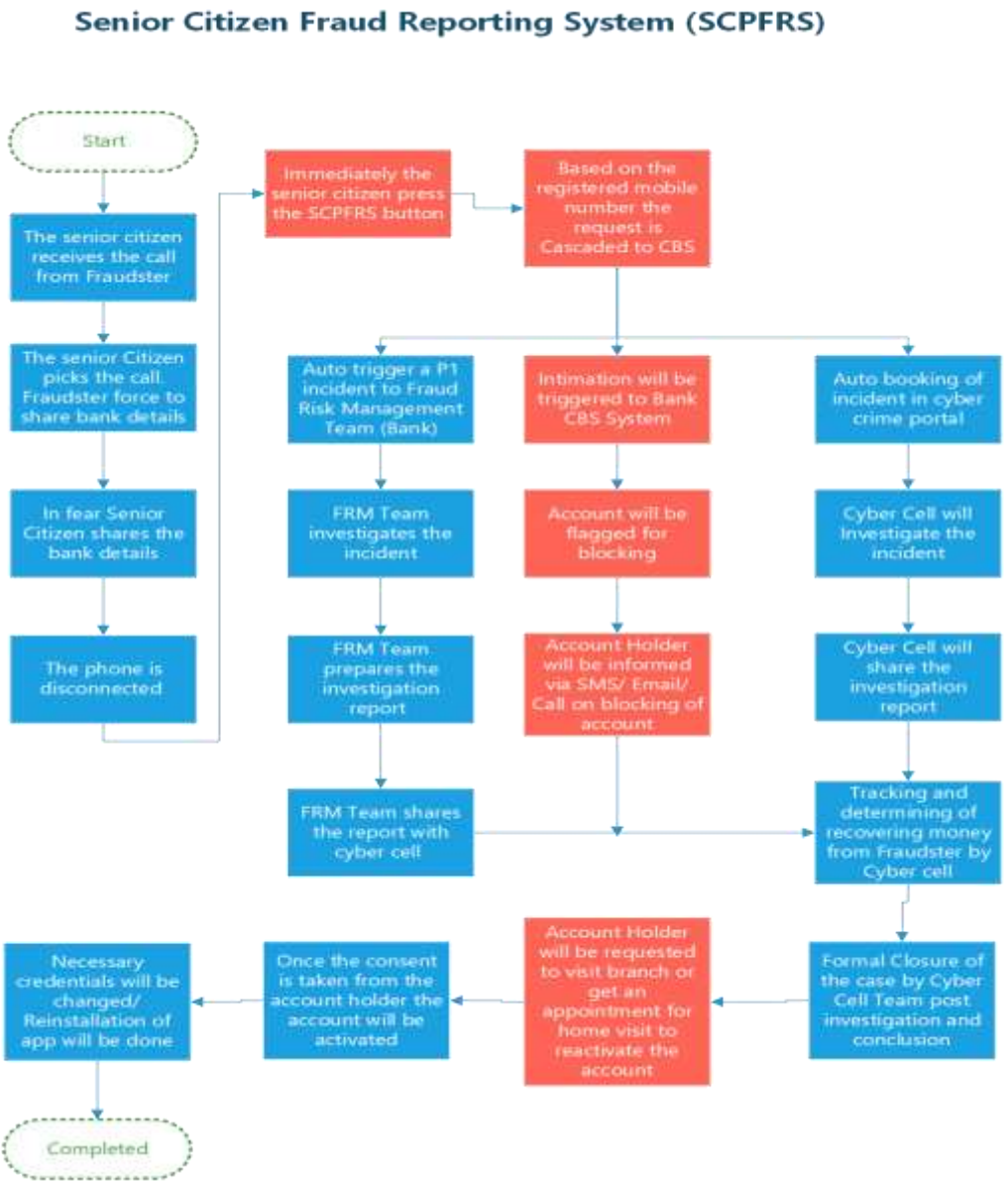
- A quick and easy action to stop money flowing out.
- It overcomes the scenario of no further transactions even if the fraudster has bank account information.

Key Takeaways

- Less efforts for the senior citizen fight against fraudster
- Bank as an entity together with cybercrime cell could help in reducing the damage to money.
- Automation can help in easy way to reduce turnaround time in registering the complaint.
- Probability of already transacted money could be recovered.

Recommendations for adoption across banks

All the banks can integrate help in reducing the online frauds by this way and at the same time this will help the cyber cell to track and instantly recover money and reach the fraudster.



Conclusion

The Senior Citizen Priority Fraud Reporting System represents a practical, technology-driven intervention aimed at minimizing financial losses during cyber fraud incidents. By enabling rapid response during the Golden Hour, the system improves fund recovery probability and reinforces customer trust in digital banking.

References

1. Lalantika Arvind, Vikash Gautam and Vrinda Maheshwari (2025), “Understanding Senior Citizens' Experience with Online Fraud”, https://saferinternetindia.com/wp-content/uploads/2025/03/Digital_Understanding-Senior-Citizens-Experience-with-Online-Fraud-A-Survey-Based-Assessment_compressed-1-2.pdf
2. Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576-586.
3. Srinath Vudali (2025), “Scammed? ‘Golden Hour’ call to cyber helpline can save money, spare your grief”, https://timesofindia.indiatimes.com/city/hyderabad/scammed-golden-hour-call-to-cyber-helpline-can-save-money-spare-you-grief/articleshow/117702835.cms

Annexure I

- Why are the senior citizens becoming the favourite victims?
- How are the senior citizens handling the trauma during the entire episode?
- How could the senior citizen financial fraud reporting system would help?
- How would the collaboration between the bank and the cybercrime cell would reduce the turnaround time to reach the Fraudster using the senior citizen financial fraud reporting system?
- What is the goal that we are achieving?

☯☯☯