FRAUD PATHWAYS TO FAIR CYBER PROTECTION: BUILDING A VICTIM-CENTRED FRAMEWORK FOR REPORTING, EVIDENCE PRESERVATION, AND INSTITUTIONAL RESPONSE

Rachita Menon, BBA LLB (Hons.), MIT-WPU School of Law

ABSTRACT

Cyberfraud is commonly framed as the consequence of victim carelessness, yet many fraud schemes succeed through carefully designed manipulation involving urgency, impersonation, authority, fear, and trust. This article develops a victim-centred framework for post-fraud reporting, digital-evidence preservation, institutional coordination, and victim protection in India. Drawing on victimology, procedural justice, cybercrime research, and oU̓icial Indian reporting and cybersecurity mechanisms, it argues that cyberfraud should be understood as a staged victimisation process rather than a single mistaken transaction. The proposed framework links immediate reporting, transaction intervention, evidence preservation, institutional referral, transparent communication, and protection against repeat victimisation. It further distinguishes effective response from guaranteed financial recovery, emphasising accessibility, timeliness, dignity, evidentiary integrity, and procedural fairness as independent measures of institutional performance. The article concludes that fair cyber protection requires not only stronger technical safeguards, but also coordinated institutions capable of reducing victim-blaming, preserving evidence, and responding rapidly after fraud occurs.

CONTEXT AND RATIONALE:

India's rapid digital transformation has significantly increased the use of online banking, Unified Payments Interface (UPI), digital wallets, e-commerce, and mobile payment applications. These technologies have improved convenience and financial inclusion, but they have also created new opportunities for cyber fraud. As digital transactions become a part of everyday life, cyber fraud has emerged as a major challenge affecting individuals, businesses, and financial institutions across the country.

Public discussions often explain cyber fraud by suggesting that victims were careless or lacked digital awareness. Although awareness is important, such explanations oversimplify the nature of modern cyber fraud. Most frauds succeed because criminals deliberately manipulate trust, authority, urgency, and fear rather than exploiting technical ignorance alone. Fraudsters impersonate bank officials, government agencies, customer support executives, or trusted organisations to convince victims that their requests are genuine. Victims frequently act under pressure, believing they are protecting their accounts or complying with legitimate instructions. Their actions result from deception rather than informed choice.

The consequences of cyber fraud extend beyond financial loss. Victims commonly experience panic, embarrassment, shame, anxiety, and uncertainty immediately after discovering the fraud. These emotional reactions often delay reporting because victims fear criticism or believe that nothing can be done. Unfortunately, delayed reporting reduces opportunities to preserve digital evidence, initiate transaction intervention, and coordinate institutional responses while financial trails remain active.

For this reason, cyber protection should not be limited to fraud prevention. Although awareness campaigns and cybersecurity measures remain essential, fraud cannot always be prevented. Institutions must therefore focus equally on what happens after a fraud occurs. Victims should have access to simple reporting mechanisms, clear guidance on preserving evidence, and coordinated institutional support that responds quickly and fairly.

Within India, post-fraud response involves several institutions, including banks, payment service providers, telecom operators, online platforms, cyber police, the National Cyber Crime Reporting

Portal (NCRP), the 1930 Cyber Helpline, the Indian Cyber Crime Coordination Centre (I4C), and CERT-In. Each institution performs a different role, making coordination essential. When victims are required to navigate multiple agencies without guidance, delays increase and confidence in the justice system declines.

This article argues that cyber protection should move beyond prevention and adopt a victim-centred framework that integrates reporting, evidence preservation, transaction intervention, institutional coordination, and procedural fairness. Such an approach strengthens both investigations and public trust while recognising that fair treatment is as important as rapid action.

RESEARCH QUESTION AND AIM:

Research Question

How can a victim-centred approach improve reporting, digital evidence preservation, and institutional response to cyber fraud in India?

Aim

This article aims to develop a victim-centred framework that explains how timely reporting, immediate evidence preservation, transaction intervention, and coordinated institutional action can strengthen post-fraud cyber protection in India. The framework seeks to promote procedural fairness, improve institutional coordination, and support victims without creating unrealistic expectations of guaranteed financial recovery.

CONCEPTUAL LENS:

This article adopts a victim-centred perspective supported by the principles of victimology and procedural justice. Rather than treating cyber fraud as a single financial transaction caused by carelessness, it views fraud as a process of deliberate psychological manipulation that continues beyond the initial loss. Victims experience not only financial harm but also emotional distress, uncertainty, and procedural challenges while interacting with multiple institutions.

The concept of procedural justice suggests that people are more likely to trust institutions when they are treated with dignity, fairness, transparency, and respect. In cyber fraud cases, this

means that victims should receive clear information, accessible reporting channels, timely updates, and realistic guidance regarding investigations and recovery. Fair treatment does not eliminate the need for verification but ensures that victims are supported throughout the reporting process.

The article also recognises that cyber fraud investigations depend on different forms of digital evidence. Victim-side evidence, such as screenshots, transaction receipts, emails, and call records, complements institution-held evidence maintained by banks, payment service providers, telecom operators, and online platforms. In some cases, investigators also rely on digital forensic evidence collected through authorised forensic procedures. Effective cyber protection therefore depends upon cooperation between victims and institutions rather than the actions of any single organisation.

CYBER FRAUD PATHWAYS AND VICTIMISATION:

Cyber fraud should be understood as a process of victimisation rather than a single financial transaction. The actual transfer of money is only one stage in a carefully planned sequence designed to manipulate victims into making decisions they would not normally make. Viewing cyber fraud in this way shifts attention from blaming victims to understanding how offenders exploit trust, urgency, and human behaviour. This perspective also highlights the importance of timely reporting, evidence preservation, and coordinated institutional action after the fraud has occurred.

The fraud pathway usually begins with trust-building. Fraudsters contact potential victims through phone calls, text messages, emails, social media platforms, messaging applications, or fake websites. They often impersonate banks, government departments, courier companies, customer support executives, employers, or even friends and family members. Their objective is to create a sense of legitimacy before requesting sensitive information or financial action.

Once trust has been established, fraudsters create a sense of urgency. Victims may be informed that their bank account will be blocked, a suspicious transaction has been detected, KYC details need immediate updating, or a refund is waiting to be processed. Some scams exploit emotions by claiming that a family member is in danger or by offering attractive investment opportunities that are available only for a limited time. These tactics pressure victims to act quickly without verifying the information.

The next stage involves manipulation and financial extraction. Victims may be persuaded to share one-time passwords (OTPs), banking credentials, card details, approve fraudulent UPI requests, scan malicious QR codes, install remote access applications, or transfer money to fraudulent accounts. In many cases, victims genuinely believe they are protecting their accounts or completing a legitimate transaction. Their actions are therefore the result of deception rather than informed consent. After the money has been transferred, fraudsters attempt to delay detection. They may assure victims that refunds are being processed or that technical problems are causing temporary delays. During this period, the stolen funds are often transferred rapidly through multiple accounts, including mule accounts, making financial tracing increasingly difficult. This demonstrates why every minute after the fraud is discovered is important for transaction intervention and evidence preservation.

Cyber fraud also creates significant emotional and psychological harm. Victims often experience panic, fear, embarrassment, confusion, and anxiety immediately after realising they have been deceived. These reactions frequently delay reporting because victims fear criticism or believe that the money cannot be recovered. Unfortunately, delayed reporting reduces the chances of preserving digital evidence and limits the ability of institutions to respond effectively.

It is also important to distinguish between repeat victimisation and secondary victimisation. Repeat victimisation occurs when fraudsters target victims again, often pretending to be recovery agents or officials who promise to return the lost money in exchange for additional payments. Secondary victimisation occurs when victims experience further harm because of insensitive treatment, repeated referrals, poor communication, or unnecessary delays during the reporting and investigation process. Both forms of victimisation reduce public confidence in digital systems and discourage future reporting.

Understanding cyber fraud as a pathway rather than a single incident demonstrates that effective cyber protection must continue after the financial loss. It requires immediate reporting, preservation of digital evidence, coordinated institutional action, and fair treatment of victims throughout the response process.

VICTIM CENTRED REPORTING:

Reporting is the first and most important step in the post-fraud response because it connects

victims with the institutions responsible for financial intervention, evidence preservation, and investigation. However, victim-centred reporting is more than simply submitting a complaint online. It recognises that victims often approach authorities while experiencing panic, confusion, shame, and uncertainty. A fair reporting system should therefore support victims while collecting the information needed for an effective response.

Immediately after discovering a fraud, victims may not know whether they should contact their bank, the 1930 Cyber Helpline, the National Cyber Crime Reporting Portal (NCRP), or the cyber police. Clear reporting channels are therefore essential. Easy access to reporting mechanisms reduces delays and allows institutions to begin transaction intervention and evidence preservation as early as possible. Victim-centred reporting should also encourage the immediate preservation of digital evidence. Victims should be advised to retain screenshots, transaction IDs, payment receipts, SMS messages, emails, call records, chat histories, account details, QR codes, and website links. These records help investigators reconstruct the fraud pathway and support financial institutions in tracing transactions. Providing victims with a simple evidence checklist at the reporting stage can prevent important information from being lost.

Effective reporting also depends on institutional coordination. Cyber fraud cases often involve banks, payment service providers, telecom operators, online platforms, cyber police, the Indian Cyber Crime Coordination Centre (I4C), and other authorities. A victim should not have to navigate these institutions independently. Instead, information should be shared efficiently between relevant organisations while victims receive clear guidance about the progress of their complaint. Victims should also receive realistic recovery guidance. Prompt reporting increases the possibility of transaction intervention and financial tracing, but it does not guarantee that stolen money will always be recovered. Honest communication regarding legal procedures, investigation timelines, and institutional limitations helps build public trust and prevents unrealistic expectations.

Finally, victim-centred reporting should protect individuals from secondary fraud. Criminals often contact victims again by pretending to be police officers, bank officials, lawyers, or recovery agents who promise to recover lost funds for a fee. Institutions should warn victims that legitimate authorities will never ask for payment to recover stolen money or request confidential banking information after a complaint has been registered.

Victim-centred reporting therefore combines empathy with efficiency. It recognises the emotional impact of cyber fraud while ensuring rapid reporting, evidence preservation, institutional coordination, realistic guidance, and protection from further victimisation. By shifting the focus from victim-blaming to victim support, reporting becomes the foundation of a fair and effective cyber protection system.

DIGITAL EVIDENCE PRESERVATION:

Digital evidence preservation is a vital part of cyber fraud response because it supports financial tracing, criminal investigation, and institutional decision-making. Unlike conventional crimes, cyber fraud leaves behind electronic records rather than physical evidence. These records help investigators understand how the fraud occurred, identify the movement of funds, and establish communication between victims and offenders. Preserving this information immediately after discovering the fraud increases the effectiveness of institutional response and reduces the risk of important evidence being lost. Digital evidence can be divided into three categories: victim-side evidence, institution-held evidence, and forensically acquired evidence.

Victim-side evidence includes information that victims can preserve themselves immediately after the incident. This may include screenshots of messages, emails, SMS alerts, payment receipts, UPI transaction IDs, bank notifications, QR codes, call records, chat histories, website links, and account details. Victims should avoid deleting conversations, uninstalling applications, formatting devices, or changing account information before preserving these records, as doing so may destroy valuable evidence. Institution-held evidence consists of records maintained by organisations involved in digital transactions. Banks retain account statements, beneficiary account details, transaction histories, and payment records. Payment service providers preserve transaction logs, timestamps, and payment references, while telecom operators maintain communication records and subscriber information.

Online platforms also store login histories, IP addresses, account activity, and communication records.

These records play an essential role in tracing fraudulent transactions and identifying offenders, but they can only be accessed by authorised institutions during the investigation.

The third category is forensically acquired evidence, which is collected by trained investigators

using legally recognised digital forensic methods. This may include device images, metadata, deleted files, malware analysis, browser history, and application logs. Such evidence requires specialised expertise and must be collected carefully to maintain its authenticity and legal admissibility. The value of digital evidence depends largely on speed. Fraudsters often transfer stolen funds through multiple accounts within minutes, while electronic records may be modified or deleted over time. Immediate reporting allows banks and payment service providers to begin transaction intervention and preserve transaction records before critical information disappears. Early evidence preservation also strengthens investigations by enabling authorities to reconstruct the fraud pathway accurately.

However, preserving digital evidence should not create unrealistic expectations regarding financial recovery. While timely evidence improves the chances of tracing fraudulent activity and supporting legal proceedings, it cannot guarantee that stolen funds will always be recovered. Its primary purpose is to protect the integrity of the investigation and ensure that institutions have reliable information on which to act.

Thus, digital evidence preservation is not simply a technical requirement but a shared responsibility between victims and institutions. When evidence is preserved quickly and accurately, it improves coordination, strengthens investigations, and supports a fair and transparent cyber fraud response.

INSTITUTIONAL RESPONSE: POLICE, BANK, PLATFORM AND CERT-Ins:

An effective response to cyber fraud requires coordinated action among multiple institutions rather than reliance on a single organisation. Each institution performs a distinct role, and the success of the overall response depends on how efficiently they work together. A victim-centred approach therefore emphasises coordination, timely communication, and clearly defined responsibilities.

The first point of contact for many victims is their bank or payment service provider. Once informed of the fraud, these institutions can record the complaint, verify transaction details, and initiate transaction intervention, where possible. Quick action is important because fraudulent funds are often transferred through several accounts within a short period. Although banks cannot guarantee recovery of money, early intervention may improve the possibility of tracing or temporarily restricting suspicious transactions.

Payment service providers, including UPI platforms and digital wallet operators, maintain electronic records such as transaction IDs, timestamps, payment references, and beneficiary details. These records assist investigators in tracing financial transactions and identifying the movement of funds across different accounts. Close coordination between banks and payment providers is therefore essential during the initial stages of investigation.

Telecom service providers also contribute by preserving communication records linked to fraudulent phone calls, SMS messages, SIM-swap incidents, and subscriber information. Since many frauds begin through mobile communication, these records can provide valuable evidence regarding the methods used by offenders.

Similarly, online platforms play an important role when fraud involves fake websites, social media accounts, online marketplaces, or impersonation profiles. These platforms can preserve account activity, remove fraudulent content, and cooperate with authorised agencies during investigations, helping prevent further victimisation.

In India, victims can report cyber financial fraud through the 1930 Cyber Helpline and the National Cyber Crime Reporting Portal (NCRP), both functioning under the Indian Cyber Crime Coordination Centre (I4C). These reporting mechanisms enable complaints to reach relevant institutions quickly and support coordination between financial institutions, cyber police, and other agencies. Prompt reporting through these channels improves the possibility of transaction intervention and evidence preservation.

Cyber Police are responsible for investigating cyber fraud offences. Their duties include registering complaints, collecting evidence, coordinating with financial institutions and service providers, tracing offenders, and initiating legal proceedings where necessary. Throughout the investigation, victims should receive clear information about procedures, documentation requirements, and available grievance mechanisms to ensure transparency and procedural fairness.

The role of CERT-In is different from that of banks or law enforcement agencies. CERT-In is India's national agency for responding to cybersecurity incidents and providing technical support, advisories, and coordination in matters affecting cyber infrastructure. While CERT-In contributes valuable technical expertise, it is not the primary authority for reporting or investigating financial cyber fraud. Recognising these distinct responsibilities prevents

confusion and strengthens institutional coordination.

Ultimately, fair cyber protection depends on cooperation among all these institutions. Banks, payment service providers, telecom operators, online platforms, I4C, cyber police, and CERT-In each contribute to different stages of the response process. When information is shared efficiently and responsibilities are clearly defined, victims receive quicker assistance, investigations become more effective, and public confidence in digital systems is strengthened.

BUILDING THE CYBER PROTECTION FRAMEWORK:

Cyber fraud is a continuous process of victimisation, and the institutional response should be equally systematic. Based on the discussion in this article, a Fair Cyber Protection Framework is proposed to guide post-fraud response. The framework places victims at the centre while ensuring that institutions work together in a coordinated and transparent manner. The framework begins when a victim recognises the fraud and immediately reports it to the bank, the 1930 Cyber Helpline, or the National Cyber Crime Reporting Portal. Prompt reporting enables institutions to begin transaction intervention, preserve financial records, and reduce the possibility of further movement of stolen funds.

The next stage involves digital evidence preservation. Victims preserve screenshots, transaction receipts, messages, emails, call records, and payment references, while banks, payment service providers, telecom operators, and online platforms secure their own electronic records. This combination of victim-side and institution-held evidence provides investigators with a complete picture of the fraud.

Once evidence has been secured, institutional coordination becomes essential. Banks, cyber police, I4C, payment providers, telecom operators, and online platforms exchange relevant information within their legal responsibilities. Effective communication reduces duplication of work, speeds up investigations, and prevents victims from repeatedly approaching different organisations.The framework also emphasises procedural fairness. Victims should receive respectful treatment, clear explanations of investigative procedures, regular updates, and realistic information regarding recovery. Institutions should avoid victim-blaming and recognise that emotional distress often affects victims' ability to respond immediately after the fraud.

Another important element is protection against repeat victimisation. Victims should be informed that fraudsters may contact them again pretending to be recovery agents, police officers, lawyers, or bank officials. Awareness of these follow-up scams helps prevent further financial loss.Finally, institutions should review completed cases to identify emerging fraud patterns, improve reporting systems, strengthen coordination, and enhance public awareness. Continuous learning allows the cyber protection framework to evolve alongside changing fraud techniques. This framework demonstrates that fair cyber protection is not measured only by financial recovery. Its success also depends on rapid reporting, effective evidence preservation, coordinated institutional action, transparent communication, procedural fairness, and continued protection of victims throughout the post-fraud process.

RISK, LIMITS AND MISUSE:

Although a victim-centred cyber protection framework can improve the response to cyber fraud, it also faces several practical and legal challenges. One of the biggest limitations is the speed at which fraudsters transfer stolen money. Funds are often moved through multiple accounts, including mule accounts, within minutes, making recovery increasingly difficult. Even when victims report incidents promptly, financial recovery cannot always be guaranteed.

Another challenge is delayed reporting. Victims often experience panic, shame, fear, or confusion immediately after discovering the fraud. These emotions may prevent them from contacting banks, cyber police, or the 1930 Cyber Helpline quickly. Such delays reduce the effectiveness of transaction intervention and may result in the loss of valuable digital evidence. Institutions should therefore recognise these emotional responses as natural consequences of victimisation rather than signs of negligence. The framework must also address the possibility of false or malicious complaints. Financial institutions and law enforcement agencies have a responsibility to verify every complaint before taking action, such as freezing accounts or initiating legal proceedings. Fair cyber protection requires balancing victim support with due process so that innocent individuals are not wrongly affected. Privacy and data protection are equally important. Cyber fraud investigations require information sharing among banks, payment service providers, telecom operators, online platforms, and law enforcement agencies. Such cooperation should be carried out only in accordance with applicable laws to protect victims' personal and financial information while supporting effective investigations.

A further concern is secondary fraud. Criminals often contact victims again by pretending to be recovery agents, lawyers, police officers, or bank officials, offering to recover lost money

in exchange for additional payments. Victims should therefore be informed that genuine authorities never demand payment for recovering stolen funds. Despite these challenges, a victim-centred approach remains valuable because it promotes timely reporting, evidence preservation, coordinated institutional action, and transparent communication. Rather than guaranteeing financial recovery, it seeks to ensure that victims receive fair treatment and that institutions respond efficiently and responsibly.

CONCLUSION:

Cyber fraud is more than a financial offence; it is a process of engineered victimisation that exploits trust, urgency, fear, and human behaviour. Viewing cyber fraud only as a result of victim carelessness ignores the sophisticated methods used by offenders and discourages victims from reporting incidents promptly. A victim-centred perspective recognises that victims require timely support, clear guidance, and coordinated institutional action rather than blame.

This article has shown that effective cyber protection extends beyond preventing fraud. Once fraud has occurred, immediate reporting, transaction intervention, digital evidence preservation, and cooperation among banks, payment service providers, cyber police, the National Cyber Crime Reporting Portal, the 1930 Cyber Helpline, the Indian Cyber Crime Coordination Centre (I4C), online platforms, telecom providers, and CERT-In become essential for supporting investigations and protecting victims. The proposed Fair Cyber Protection Framework demonstrates that institutional success should not be measured solely by the recovery of stolen money. Equally important are the accessibility of reporting mechanisms, the preservation of digital evidence, timely institutional coordination, transparent communication, procedural fairness, and protection from repeat victimisation. These factors strengthen public trust in the cyber justice system even when complete financial recovery is not possible.

As India's digital economy continues to expand, cyber fraud will remain an evolving challenge. Strengthening post-fraud response through victim-centred policies, better institutional coordination, and improved evidence preservation will contribute to a more resilient and trustworthy digital environment. Fair cyber protection is therefore not only about responding quickly but also about responding fairly, responsibly, and with the needs of victims at the centre of every stage of the process.

REFERENCES:

1. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2013). *Measuring the cost of cybercrime*. Springer.

2. Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger.

3. Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims. *Security Journal, 27*(1), 36–54.

4. Cross, C., Richards, K., & Smith, R. G. (2016). Improving responses to online fraud victims. *Trends & Issues in Crime and Criminal Justice*, 518, 1–15.

5. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and digital forensics*. Routledge.

6. Indian Computer Emergency Response Team. (2022). *Directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents*. Ministry of Electronics and Information Technology.

7. Indian Cyber Crime Coordination Centre. (2023). *Annual Report*. Ministry of Home Affairs. 8. Ministry of Home Affairs. (2023). *National Cyber Crime Reporting Portal*. Government of India.

9. National Crime Records Bureau. (2023). *Crime in India 2022*. Government of India.

10. National Payments Corporation of India. (2024). *UPI Procedural Guidelines*. NPCI.

11. Reserve Bank of India. (2024). *Annual Report 2023–24*. RBI.

12. Reserve Bank of India. (2024). *Master Directions on Digital Payment Security Controls*. RBI.

13. United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*. United Nations.

14. Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

15. Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). Sage.

16. Government of India. (2023). *Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)*. Ministry of Home Affairs.