TAXONOMISING DIGITAL FINANCIAL FRAUDS FOR ECOSYSTEM RESILIENCE

aapti institute

DEEPSTRAT
STRATEGY . POLICY . ACTION

Supported by IIMA VENTURES

Authors

Aditi Shah | **Aapti Institute**

Astha Kapoor | **Aapti Institute**

Mousmi Panda | **Aapti Institute**

Rihan Shareef | **Aapti Institute**

Partners

Anand Venkatanarayanan | **DeepStrat**

Saikat Datta | **DeepStrat**

Supported by

Supriya Sharma | **IIMA Ventures**

Vijeth Acharya | **IIMA Ventures**

Trisha Ghoshal | **Independent Consultant**

Samvegi Shah | **IIMA Ventures**

Disclaimer: The case study findings presented are from independent research and direct examination of publicly accessible platform features. The analysis is intended to inform discussions on product design, user safety, and governance in the digital ecosystem. References to specific platforms are illustrative and do not imply any statement regarding intent, compliance, or negligence by the respective companies.

TABLE OF CONTENTS

CONTEXT AND SCOPE

CONTEXT AND SCOPE

A SHARP INCREASE IN DIGITAL FINANCIAL FRAUD HAS IMPLICATIONS ON HOW USERS FORM TRUST WITH PRODUCTS

Emerging research on Trust and Safety points to the conclusion that if the businesses are unable to protect consumers from digital financial fraud and misleading content, users are likely to move away from those products

> "The fear of being scammed is one of the top global barriers to trust in digital payments—nearly half of users (46%) cite it as a key concern, highlighting that scams are perceived as a risk on par with data breaches and hacking."

> Fraud perpetrators exploit trust by feigning familiarity—posing as loved ones, official agencies, or familiar brands such as WhatsApp, Facebook and Gmail—to confuse and deceive.

Despite the accelerated adoption of digital payment technologies, the widespread nature of digital financial fraud renders the maintenance and repair of user trust, a significant hurdle for products.

The term 'fraud' in this research refers to digital financial fraud and is used interchangeably throughout the study.

Sources: Chubb Report, GASA Report 2025

CONTEXT AND SCOPE

A SURGE IN DIGITAL FINANCIAL ADOPTION HAS BEEN ACCOMPANIED BY SCAMMERS EXPLOITING THEM FOR FRAUD

Emerging research on rising payment frauds highlights how vulnerabilities in the payment products are exploited, ultimately affecting the people and the fintech sector

> India's fintech market is valued at USD 44.12 billion in 2025, with digital payments accounting for 42.9% of the market in 2024.

> 57% of all fraud incidents in India are platform frauds i.e. fraudulent activities on social media, e-commerce, enterprise and fintech platforms.

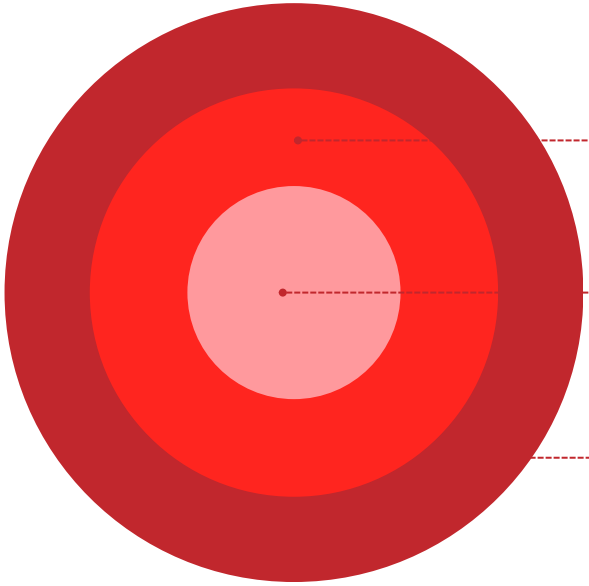
With India's fintech market set to reach USD 95.30 billion by 2030 and digital payment volumes and values growing at over 24–25% annually, the intersection of fraud, fintech, and digital payments needs closer attention.

Sources: Chubb Report, GASA Report 2025

CONTEXT AND SCOPE

A FRAGMENTED DIGITAL ECOSYSTEM BECOMES VULNERABLE TO BAD ACTORS

Perpetrators of digital financial fraud exploit cracks in user knowledge, policy efficiency, and product robustness



POLICY

Lagging in innovation,
therefore unable to keep up, and is insufficient

PRODUCT

Building narrow trust with users,
not invested in trust ecosystem maintenance or repair

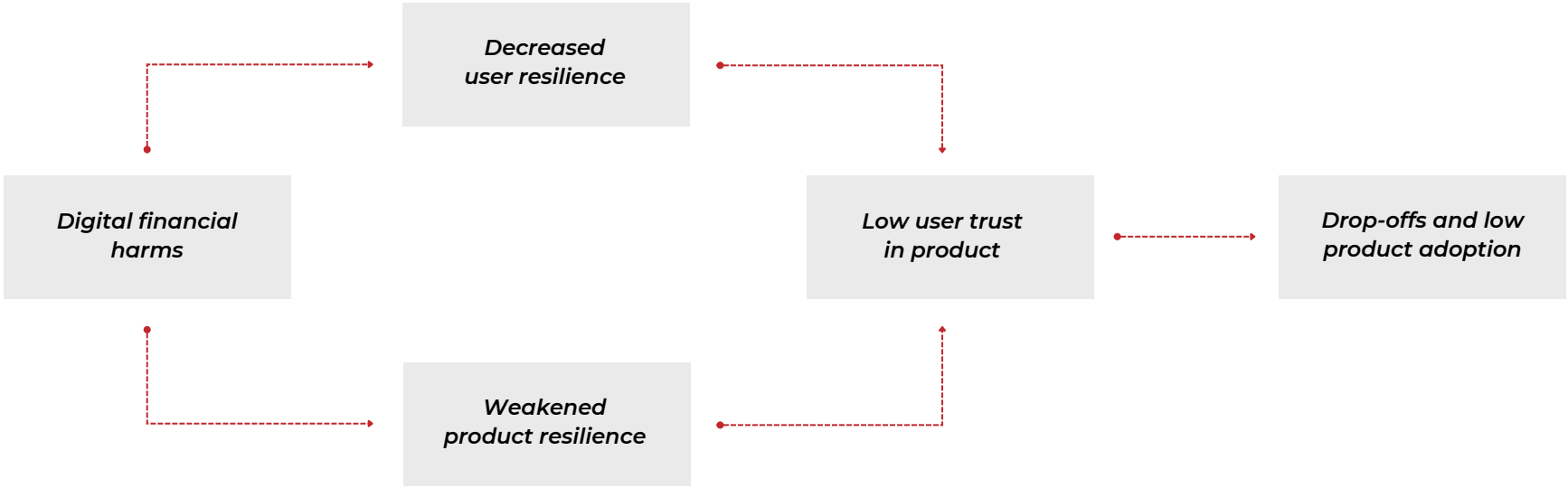
PEOPLE

Unaware, and lack tools, therefore avoidant and unable to protect themselves

CONTEXT AND SCOPE

FRAUD IS A “MONETIZABLE” MANIFESTATION OF VULNERABILITY, WHICH HAS IMPLICATIONS FOR USER TRUST

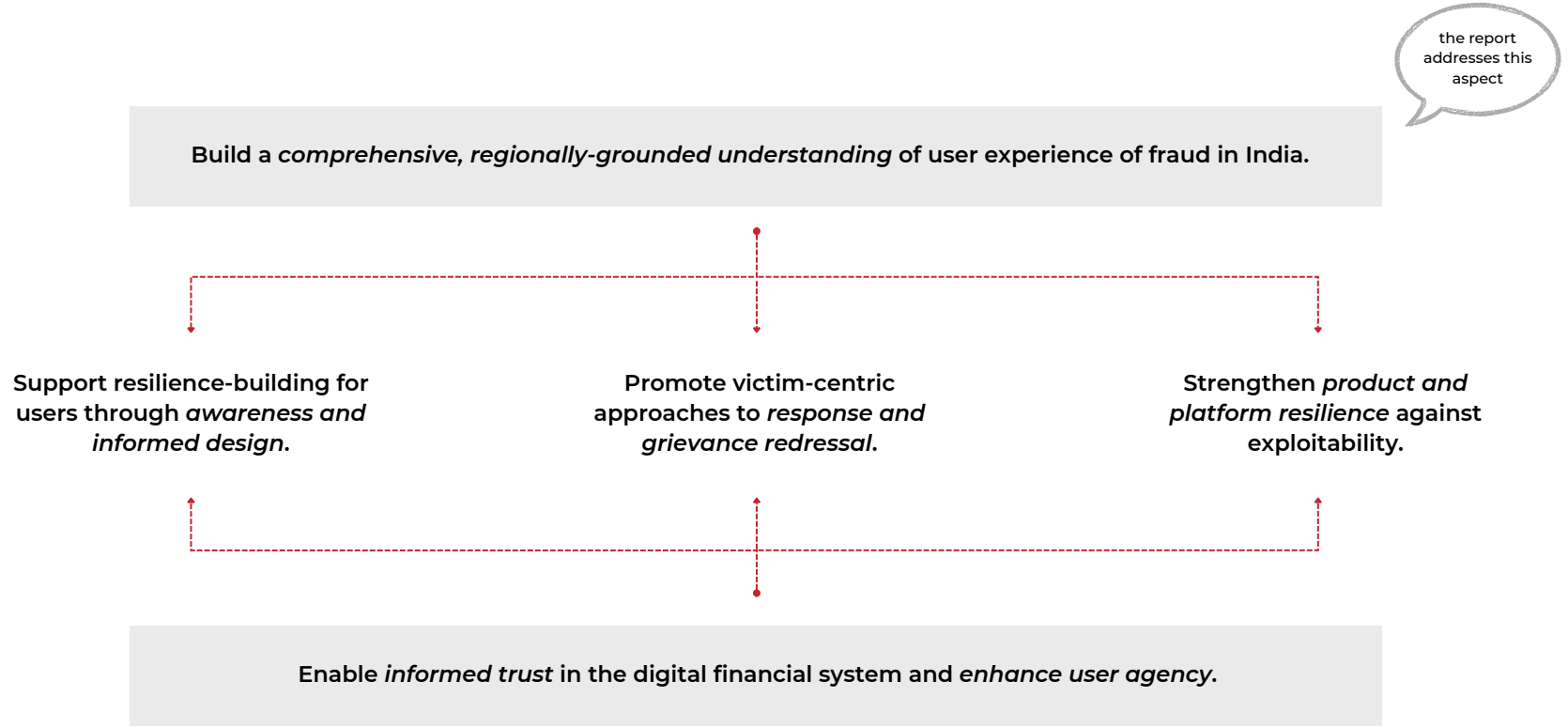
With users, perpetrators of fraud turn passive digital risk into active harm by exploiting emotional vulnerabilities and gaps in knowledge



CONTEXT AND SCOPE

BY BETTER UNDERSTANDING ECOSYSTEM VULNERABILITIES, WE CAN CHART PATHWAYS TO FRAUD PREVENTION AND RESPONSE

This work attempts to taxonomise digital financial harms and the ecosystem vulnerabilities exploited to enact them



CONTEXT AND SCOPE

WE CONSOLIDATE THREE OUTPUTS FOR A COMPREHENSIVE, FOUNDATIONAL UNDERSTANDING OF DIGITAL FINANCIAL FRAUD IN INDIA

This serves as a starting point for the development of a coordinated and effective resilience strategy

Fraud Taxonomy

Structured framework that categorizes digital financial fraud by interaction stage, perpetrator tactics, and user and product-related vulnerabilities across digital ecosystems

Victim Persona Journey Maps

Mapping of victims to persona types based on the emotional and cognitive vulnerabilities exploited, and journey maps outlining stages of their interactions with fraud perpetrators

Product Case Studies

Deep dives into digital products commonly used by perpetrators to defraud victims, to identify vulnerabilities and examine the role of design choices in contributing to or mitigating fraud-related risks

METHODOLOGY

METHODOLOGY

WE USED A MIXED-METHODS APPROACH THAT CENTRED ON DATA OBTAINED VIA FIRST INFORMATION REPORT (FIR) AND THE CYBER CRIME HELPLINE

Following from this, we mapped vulnerabilities in various forms - from victim personas to product-level features

Literature Review

- Literature on the fraud landscape in India
- Systematic review of 100 newspaper articles

Data Analysis

- 298 complaints received on the 1930 helpline, pre-categorised
- Coding of 120 FIRs between 2023-2025

Ecosystem Interviews

- Interviews with three IIMA Ventures portfolio start-ups
- Expert interview with Dr. Alice Marwick

Vulnerability Mapping

- Mapping of emotional and cognitive vulnerabilities to user personas
- Mapping of design and feature-specific product vulnerabilities

METHODOLOGY

FIR DATA PROVIDES AN AUTHENTIC ENTRY POINT INTO THE EXPERIENCES OF FRAUD VICTIMS

Upon completing the analysis, the following advantages and limitations of using FIRs as a data source are revealed

Key benefits of using this data include:

Official and verified records **ensure authenticity of the data source**

Granular details **around scam type, tactics, and techniques used**

Helpful to understand ***geographical and temporal trends***

Some limitations surface:

Underreporting **due to stigma, lack of awareness, low trust in law enforcement**

Smaller value scams **receive inadequate focus, in comparison to severe or escalated cases**

Incomplete or limited updates **on the incident after the FIR is filed**

Complementing the FIR data with data sources such as complaints and secondary data, and methodologies such as expert and industry interviews helps address some of the limitations.

METHODOLOGY

HELPLINE DATA PLAYS A LARGELY SUPPLEMENTARY ROLE

The kind of data points that emerge are largely similar to information we have been able to derive from FIRs

Key benefits of using this data include:

Studying *cases that do not get converted* into FIRs

Deep insight into *key data points*

Comparing amount defrauded with amounts frozen and recovered

However, it is not as comprehensive as FIR data for the following reasons:

No information on *perpetrator MO*

Lack of *geographic diversity*

Lack of insight into *methods of vulnerability exploitation*

Although this data provides information on cases that do not get converted to FIRs, the information is of a lesser quality compared to the narrative detail present in FIRs.

LITERATURE REVIEW

LITERATURE REVIEW

THE LITERATURE REVIEW PRIORITIZED SOURCE DIVERSITY TO CAPTURE VARIOUS DIMENSIONS OF THE RESEARCH QUESTION

However, severe underreporting results in a distorted picture of the scale of the issue

SOURCE	SIGNIFICANCE
Market Research	*Understanding scale, global and national trends on fraud*
Journalistic Accounts	*Broad patterns of fraud perpetration, scope of reporting, action taken*
Law & Regulations	*Regulatory actions, challenges, and limitations*
Academic Research	*Psychological lens on vulnerability*

In addition to providing an overview, this exercise also helped further scope the research.

LITERATURE REVIEW

A GLOBAL ‘SPAMDEMIC’ HAS EMERGED, EVOLVING ACROSS USER DEMOGRAPHICS AND PAYMENT SYSTEMS

Digital financial frauds are widespread, often executed in real time and disproportionately targeting the young

Younger population is more prone **to online scams globally - While 59% of people overall know someone who has been scammed, this rises sharply to 77% among individuals aged 18–24..**

Tech support scams **target two out of three U.S. citizens.**

Real time payment authorised push payment frauds **are rising, and expected to rise from 63% in 2023 to 80% in 2028.**

As of 2024, there is an estimated loss of *around $6.1 billion* due to cyber fraud.

Digital financial fraud now impacts a vast share of the global population and economy, underscoring the scale and urgency of the threat.

LITERATURE REVIEW

INDIA'S DIGITAL LANDSCAPE ALSO REFLECTS A GROWING VULNERABILITY TO DIGITAL FINANCIAL FRAUD

However, we do not have a comprehensive understanding of its scale and nuances, at present

Lack of quality data **on victim age, and other demographic characteristics in India**

Tech support scams **marginally higher than global statistics, with 7 out of 10 Indian consumers being victim to these**

Real time payment APP frauds **are already high, with UPI driving most cases - around 89% of scams in India occur through real-time payment systems**

The India Cyber Crime Coordination Centre estimates an annual loss of *₹1.2 trillion* for Indians next year due to cyber fraud

Although mirroring global patterns, the uniqueness of the Indian digital ecosystem renders its fraud ecosystem equally, if not more, idiosyncratic, necessitating a deeper inquiry of its own.

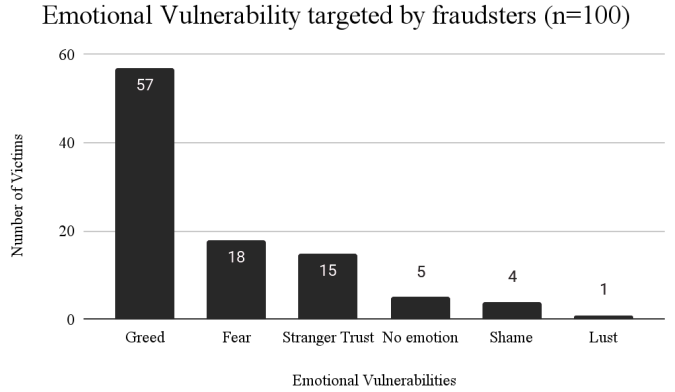
LITERATURE REVIEW

AS A PRELIMINARY EXERCISE, WE ANALYSED NEWSPAPER ARTICLES HIGHLIGHTING DIGITAL FINANCIAL FRAUD

We examined 100 articles from June 2024 to July 2025 using the search terms “cyber fraud” and “online scams”, based on a Google Trends analysis

Observations include:

40%	Investment-based scams	Most popular amongst individuals between the ages of 24 and 60, followed by those above 60
21%	Threat of legal action	Predominantly targeted towards individuals above 60
12%	Part-time jobs	Non-existent in the 60+ age category, prevalent for individuals aged 24-60



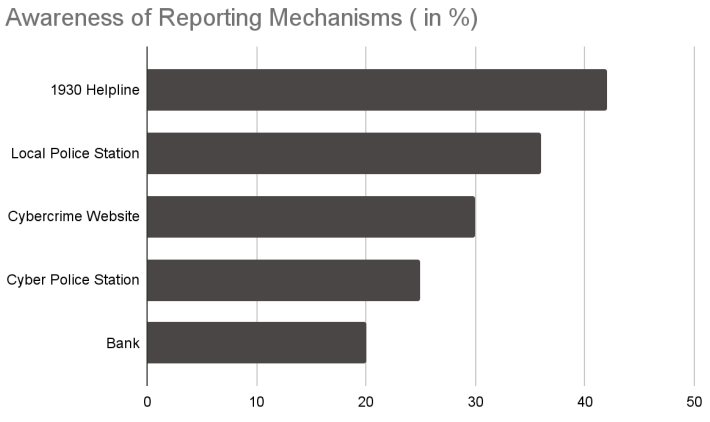
Note:
This is a preliminary categorisation based on emotions articulated in the news reporting; this was developed further in later analysis of FIRs

Source: Aapti analysis

LITERATURE REVIEW

REPORTING INFRASTRUCTURES, HOWEVER, ARE UNDER-UTILISED

On average, 6000 cases of digital fraud are reported to the 1930 helpline and on the government's online cybercrime portal per day



Note:
Users can also report through their UPI platform and NPCI, in case of UPI transactions. However this was not part of the questions in the Lokniti-CSDS Survey.

- A legal expert on cyber law estimates that only 5% of the cyber crime cases are reported.
- 51% of victims of UPI fraud did not report it to authorities.
- Only 21% of the victims of cyber fraud reported, with 76% deciding against taking formal action.

Awareness of reporting mechanisms is still low, and even those victims who are aware often do not report for various reasons, including fear and embarrassment. The actual scale of fraud in the country is therefore unknown.

Source: LokNiti-CSDS Survey

LITERATURE REVIEW

REGULATORS PLAY AN IMPORTANT ROLE IN INCREASING ECOSYSTEM RESILIENCE ACROSS THE GLOBE

Regulations are expanding to include platforms, tech-led approaches, and oversight of e-money and other sectors

United Kingdom

Provides 100% reimbursement to victims
APP (Authorised Push Payment) Reimbursement Policy 2024

Australia

Passed a bill creating sector-specific obligations to companies/platforms to prevent scams
Scams Prevention Framework (SPF) Bill 2025

European Union

Working to build a fraud-resistant, transparent and safe payment
Proposed a "comprehensive anti-fraud framework" in June 2025

Different jurisdictions have adopted distinct, targeted systemic approaches to addressing fraud-related risks and experimented with various levers of control

LITERATURE REVIEW

IN INDIA, REGULATORS ISSUE GUIDELINES IN THE FACE OF INCREASING FRAUD

Focus on regulating customer/ bank/platform liability

RBI: 2017 circular limiting customer liability on electronic fraud

NPCI: Guidelines in 2021, 2022 (a)(b), 2023 limiting customer liability for platforms with uniformed reporting procedures

Focus on regulating calls that consumers receive and call centre permissions

DoT: Several fraud perpetrators operate out of call centres requiring a licence under the 2021 Guidelines

TRAI: Telecom Commercial Communications Customer Preference (Second Amendment) Regulations, 2025

Focus on crime reporting

I4C: Nodal federal agency for law enforcement agencies, generates awareness, and manages the 1930 helpline and online cybercrime portal

Indian regulatory bodies currently focus primarily on post-fraud regulation, however TRAI has been taking steps towards prevention.

LITERATURE REVIEW

DESPITE THIS, BUSINESSES IN INDIA ARE VULNERABLE TO DIGITAL FRAUD IN TWO KEY WAYS

Fraudsters either target businesses directly or use them as vehicles for defrauding individuals

Defrauding businesses directly

- 64% of all frauds experienced in 2024 by businesses in India were cyber frauds.
- Indian fintech firm Navi was scammed for 14.26 crores due to a vulnerability in their payment gateway.
- 59% of Indian firms faced financial fraud in 2 years.
- Research estimates that Indian businesses may lose ₹20,000 crore to cybercrimes in 2025.

Defrauding businesses by impersonation

- Scamsters claim to be from RBI using fake voicemails and apps.
- Bank employee impersonation fraud through SMSes and calls.
- Imposters sending texts pretending to be from Amazon.
- Paytm KYC fraud, where perpetrators pretend to be customer care executives of the company.

While the former leads to immediate financial loss to the business, the latter results in reputational damage and notional revenue loss due to erosion of consumer trust.

LITERATURE REVIEW

GLOBAL DATA SHOWS LIMITED RESILIENCE CAPACITY RENDERS SMALL BUSINESSES UNIQUELY VULNERABLE TO FRAUD

Small businesses become targets to a range of frauds such as tech support, fake invoice, domain name, social media scams

Why it matters?

- Median loss per fraud incident: *$150,000* (ACFE)
- Small businesses face *rising fraud threats*—a 70% increase since the pandemic (Experian)
- *1 in 3 small businesses* report being defrauded; average loss ~$55,000 (Truist, 2021)

Why they are vulnerable?

- *Lack of internal controls* such as anti-fraud measures in small businesses
- *Limited resources & expertise* to detect and prevent fraud
- *High trust environments and fewer staff* lead to increased exposure

The growing vulnerability of small businesses to fraud underscores the urgent need for tailored support to strengthen awareness, resilience, and protective measures.

LITERATURE REVIEW

EARLY INSIGHTS INTO SURGE IN SMALL-BUSINESS FRAUD IN INDIA ALSO UNDERSCORE THE NEED TO FOCUS ON THEIR UNIQUE RISKS

Fraudsters shift target toward small-business accounts in india, and exploit PANs and fake Udyam certificates

Why it matters?

- **Small business are the backbone of Indian economy**
- **Fin-tech solutions *empowers* the MSMEs and boosts small businesses**

What's Lacking?

- **Focused research on fraud patterns targeting small businesses**
- ***Clearer breakdown of cybercrimes into specific types such as financial fraud and scam types***
- ***Nuanced data that captures data points: company size, sectors.***

The lack of nuanced data and information on small business fraud makes it difficult to gaze the scale of risks and develop tailored solutions

LITERATURE REVIEW

THE LITERATURE REVIEW POINTS TO THE FOLLOWING PSYCHOSOCIAL VULNERABILITIES OF INDIVIDUALS EXPLOITED BY PERPETRATORS

77% of consumers in India who lost money in 2021 reported experiencing severe or moderate levels of stress, 8% higher than the global average

Fraud perpetrators exploit...

These psychosocial vulnerabilities above are just indicative, with the taxonomy providing a more comprehensive picture of user vulnerability.

LITERATURE REVIEW

HOWEVER, GAPS IN THE LITERATURE POINT TO A NEED FOR A MORE NUANCED UNDERSTANDING OF DIGITAL FRAUD

The literature review exposes the followings gaps in existing research, which our taxonomy hopes to address

Lack of victim-centric, experiential studies **reflects a dearth of insights in terms of socio-demographic vulnerability, preventing focused action.**

Absence of a detailed taxonomy beyond broad categories **prevents us from understanding the ecosystem of actors as well as their motives and interactions with others.**

Limited insight into the exploitation of digital financial products **limits the scope for improved product design that can mitigate fraud-related risk.**

Limited insight into fraud networks, tactics, and tools **hinders the development of products that resist trust-building techniques adopted by fraud perpetrators.**

LITERATURE REVIEW

TO UNPACK THESE HARMS, WE INSPECT THE SOCIAL, DIGITAL, AND FINANCIAL CONDITIONS THAT RENDER THEM POSSIBLE

The analysis centres the following categories across the harms, actors involved, and flows between them

Harm Types and Range
Perpetrator Tactics

Victim Demographic Profile and Experience
Emotional Vulnerabilities

Financial Products Used
Product Vulnerabilities

Redressal Mechanisms
Regulatory Protections

DATA ANALYSIS

Cyber crime helpline complaints

DATA ANALYSIS

THE DATA ON COMPLAINTS TO THE CYBER CRIME HELPLINE IS COMPILED FROM SEVERAL SOURCES

The data spans less than a month, from 1st January 2025 to 20th January 2025 and is pre-classified

> ***Out of the 526 complaints received, 298 were about financial fraud.***

***From the complaints*, we got the following data:**

- → Date of complaint
- → Victim age and profession
- → Fraud type/Transaction method
- → Amount defrauded

Supplemented by *information from other sources*:

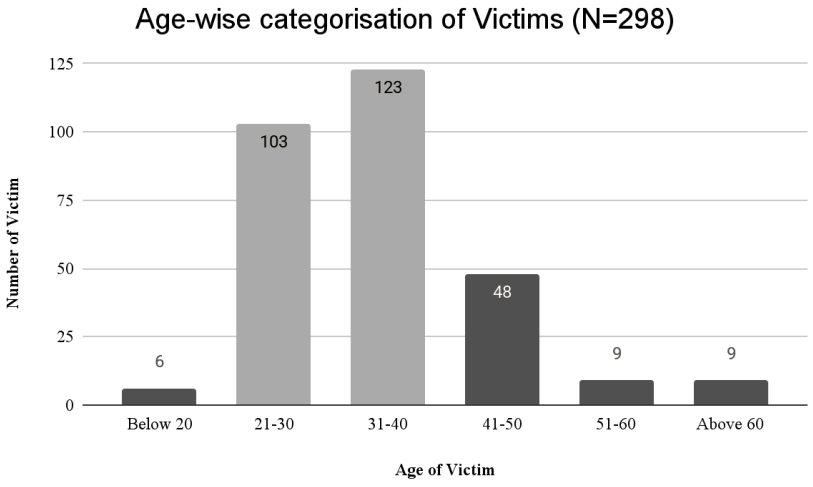
- → Frozen, held, and lien amounts
- → Amount recovered
- → Status of complaint, if disposed or converted into FIR

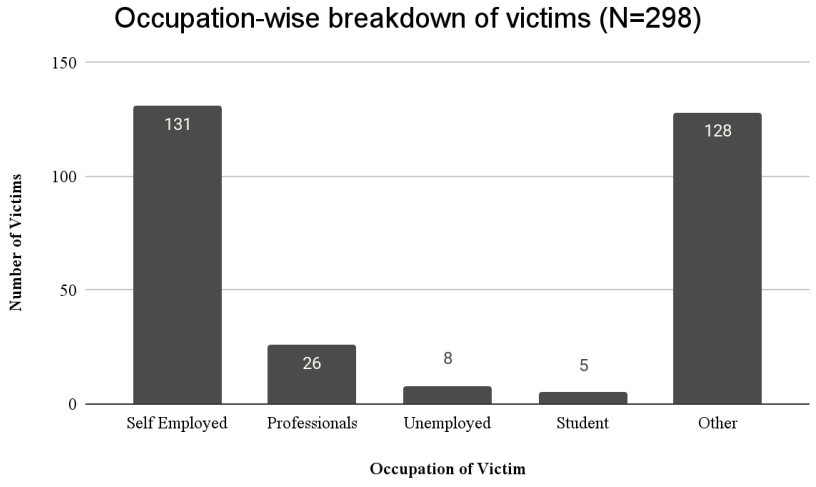
The complaints and related data provides key insights on victim demographics, conversation rates to FIRs and amount frozen/recovered

DATA ANALYSIS

THE MAJORITY OF VICTIMS WHO CALL THE HELPLINE ARE BETWEEN THE AGES OF 21 AND 40

Self-employed individuals represent the largest share, with students representing the smallest





Older victims comprise a small portion of the complaints data, which may be attributed to a lack of awareness about the helpline.

DATA ANALYSIS

FRAUD COMMITTED VIA UPI COMPRISES A THIRD OF ALL DIGITAL FRAUD REPORTED IN OUR SAMPLE

The data is pre-classified based on both the payment method and the hook used to target the victim e.g. UPI and OLX comprise separate categories in the same classification. This leads to a skewed picture of the types of fraud that are reported.

Top 5 Categories of Fraud Classification	*Number of Cases*
UPI Fraud	109
Debit/Credit Card Fraud	59
OLX/House Rent/Online Sale/Purchase/Online Advertisement Fraud	35
Internet Banking Related Fraud	15
Impersonation Oriented Fraud (Pehchan Kaun)	12

Other categories include: investment, demat or depositary, Instagram, part-time job and matrimony fraud.

The prevalence of UPI-based fraud, points to perpetrators taking advantage of its ease and convenience, and arguably of an inadequate amount of friction.

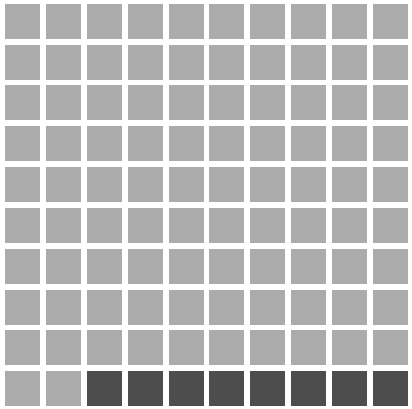
DATA ANALYSIS

OF THE COMPLAINTS RECEIVED, 3% ARE CONVERTED INTO FIRS

The two most common forms of redressal after filing a complaint are - filing an FIR for further investigation, or freezing the amount defrauded when possible. No amount has been kept as lien or been recovered

Amount De-frauded v/s Amount Frozen/On hold

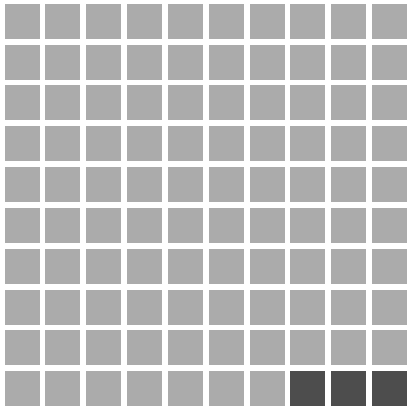
8% of the amount reported as de-frauded, get frozen/on hold by the helpline



Amount de-frauded Amount frozen/on-hold

% of complaints that have been converted into FIR's

10 out of 298 complains (3%)



Complaints not converted Complaints converted

With 89% of helpline complainants receiving no redressal, this indicates gaps in FSP follow-up and underscores the need for stronger and time-bound interventions for law free rates

DATA ANALYSIS

First Information Reports

DATA ANALYSIS

THE FIRS THEMSELVES OFFER DEEPER INSIGHT INTO THE NUANCES OF FRAUD EXECUTION, AS EXPERIENCED BY THE VICTIM

On Victims

- Age
- Gender
- Emotional vulnerabilities
- Cognitive vulnerabilities

On Tools and Techniques

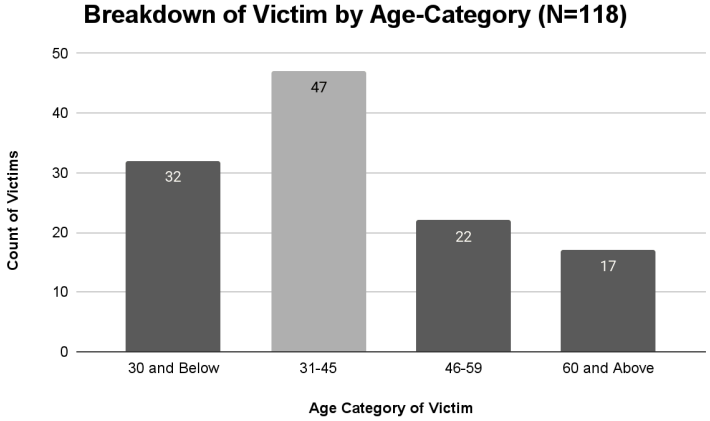
- Type of scam
- Amount lost
- Point of initial access
- How the victim lost money
- Hook that enabled the scam
- Communication channel

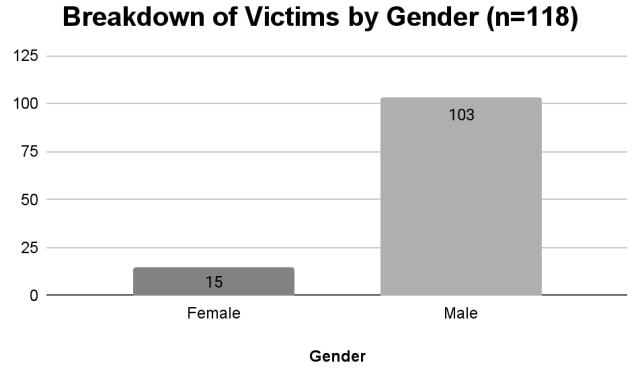
FIRs capture a significant portion of the victim-perpetrator interaction, from the point of preparation to the transaction(s) and the resulting financial, emotional, and mental impact on the victim.

DATA ANALYSIS

AN ANALYSIS OF 120 FIRS REVEALED CERTAIN SOCIO-DEMOGRAPHIC INSIGHTS ABOUT VICTIMS

Younger individuals are more likely to be victims, and complaints are overwhelmingly filed by men





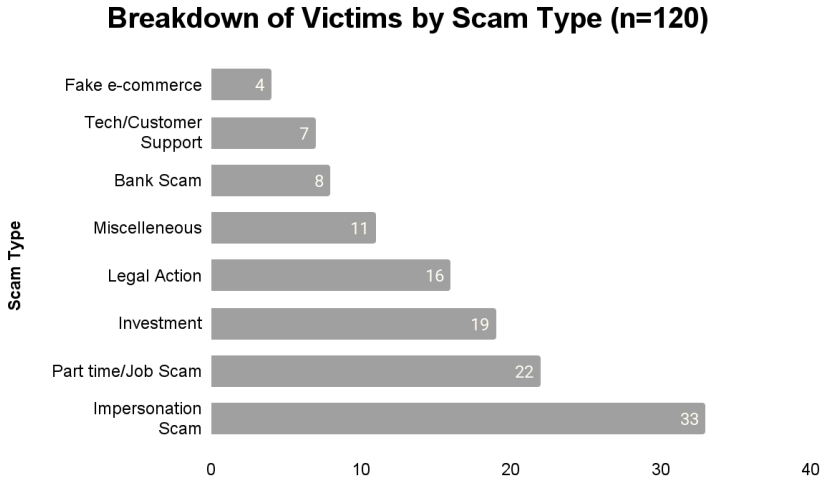
Note: 2 out of the 120 FIRs have been filed by Indian companies, hence not part of age & gender figures.

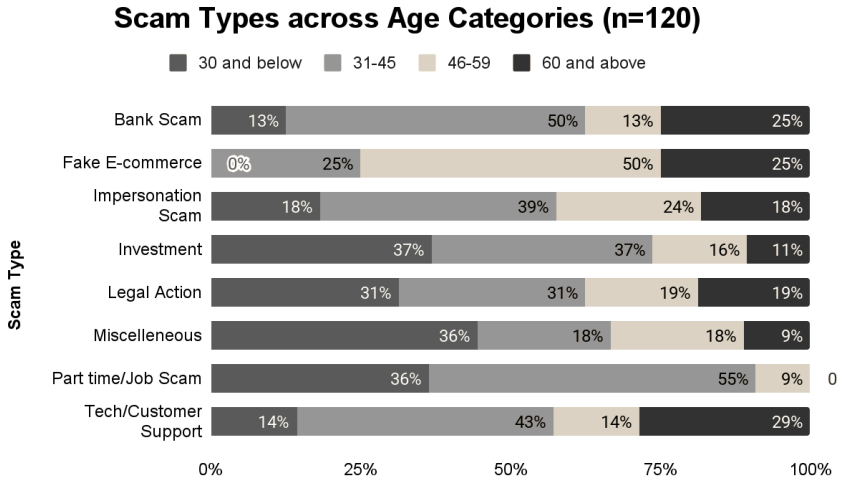
Those *under 45* are more likely to be targeted by perpetrators and report being defrauded. In terms of the gender distribution, *women* victims represented only *12%* of FIR filers.

DATA ANALYSIS

IMPERSONATION AND GET-RICH-QUICK SCAMS ARE MOST COMMON; INDIVIDUALS AGED 31-45 MOST OFTEN FALL PREY TO THE LATTER

Analysis of the FIRs based on the type of scams victims have faced, and a mapping of the same to victim age



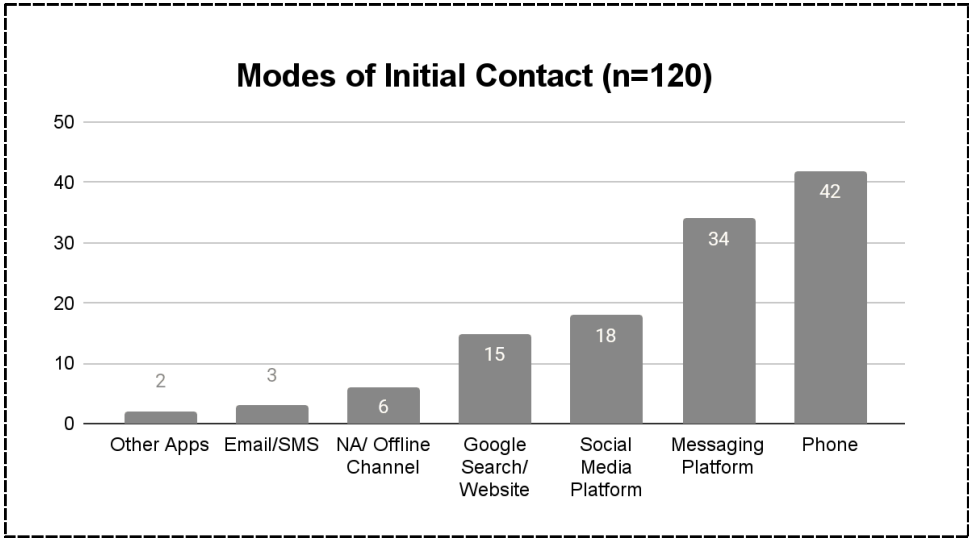


Bank-related and part-time job scams are usually aimed towards middle-aged individuals, while half of fake e-commerce scams are targeted at those between the ages of 46 and 59.

DATA ANALYSIS

PHONE CALLS AND MESSAGING PLATFORMS CONSTITUTE OVER 63% OF HOW VICTIMS ARE FIRST CONTACTED

From the initial time of contact, scams usually take place within a day



→ 278 days is the longest duration of a scam, 53% of the time a scam takes a day or lesser to execute.

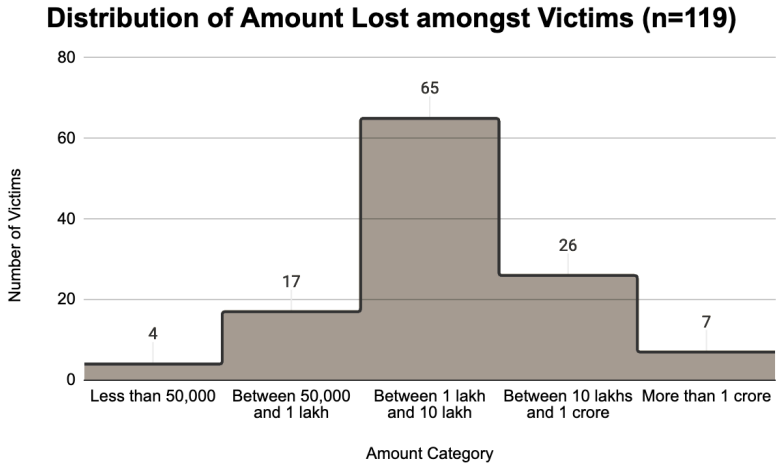
→ The total amount of money reported lost across the 120 FIRS is 19.38 crore rupees.

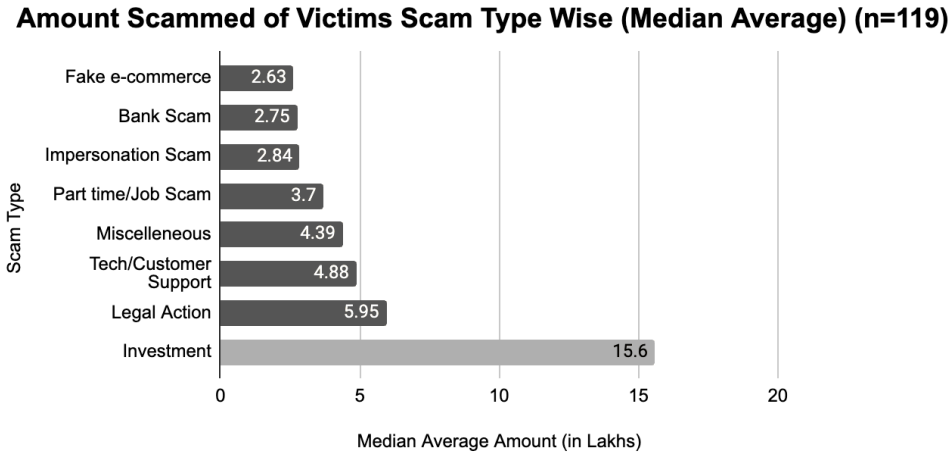
In addition to regular phone calls, messages and calls made via popular instant messaging apps are popular, low-barrier ways in which to reach out to victims.

DATA ANALYSIS

54% OF VICTIMS LOST BETWEEN 1 TO 10 LAKH RUPEES, WITH THOSE FALLING PREY TO INVESTMENT SCAMS AVERAGING A LOSS OF 15.6 LAKHS

The following graphs give insight into the money victims were defrauded of





Majority of the scams in the FIRs, are between 1 lakh and 10 lakhs, only investments scams are have a higher median average than this amount.

DATA ANALYSIS

OF THE INDIVIDUALS DEFRAUDED OF LESS THAN 10 LAKH RUPEES, 68% WERE 45 YEARS OLD OR YOUNGER

Amount category	Count of individual victims by age category					
Amount Category	***30 & Below***	***31-45***	***46-59***	***60 & Above***	***Company***	***Grand Total***
Between 1 lakh and 10 lakh	20	24	11	10		65
Between 10 lakhs and 1 crore	6	10	6	3	1	47
Between 50,000 and 1 lakh	5	10	1	2		18
Less than 50,000		2	2			4
More than 1 crore		1	2	2	1	6
NA	1					1
Grand Total	***32***	***47***	***22***	***17***	***2***	***120***

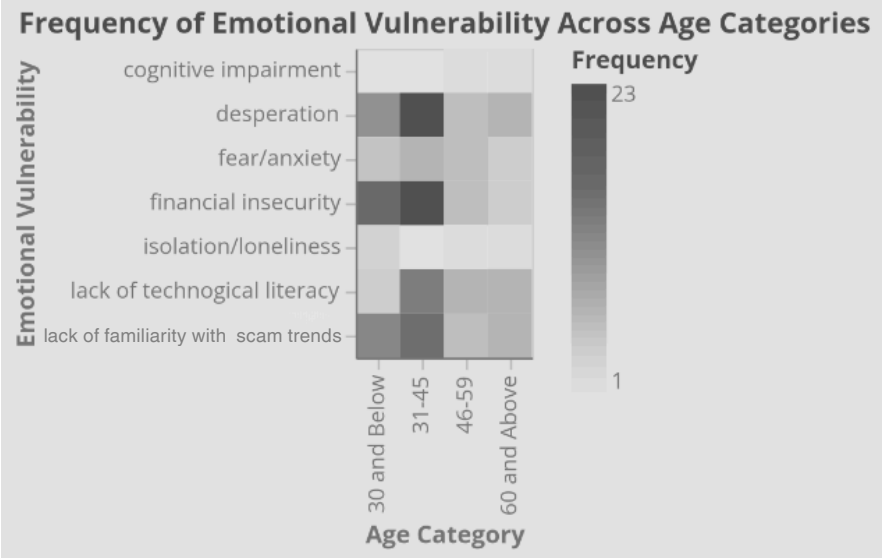
Table: Correlation of amount defrauded and age category

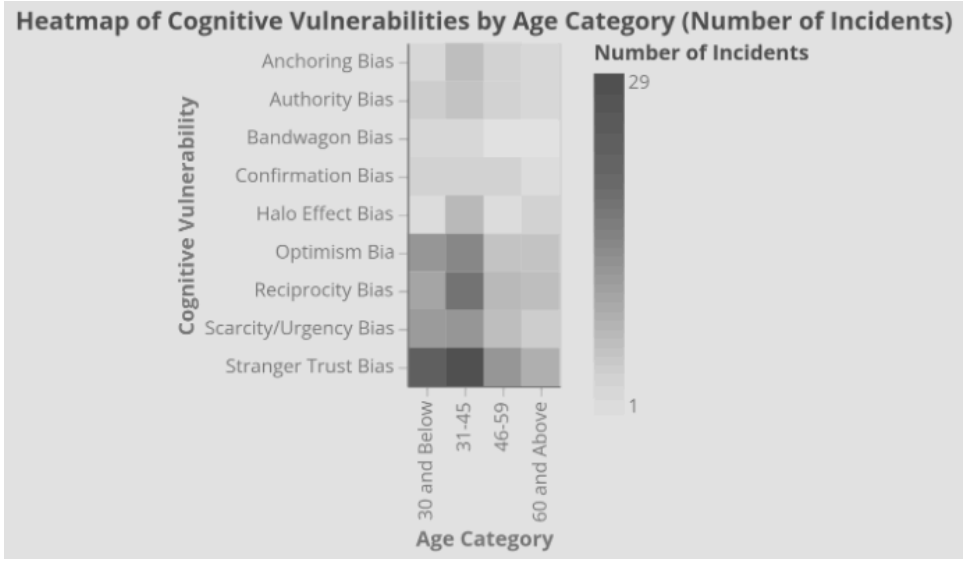
Despite age having a correlation with amount, there is an even spread of the latter across age categories. This indicates the lack of an age-specific strategy when perpetrators set amount-related targets.

DATA ANALYSIS

DESPERATION AND FINANCIAL INSECURITY ARE MOST WITNESSED IN THE 31-45 AGE GROUP, IN ADDITION TO STRANGER TRUST BIAS

Insights on emotional vulnerabilities come from the literature review and data analysis, with a detailed breakdown in the taxonomy





Desperation, financial insecurity and strange trust bias in age categories of ages 31 to 45 are the most common vulnerabilities, however several vulnerabilities span across all age groups.

DATA ANALYSIS

PERPETRATORS IMPERSONATING BANK EMPLOYEES OR LEGAL AUTHORITIES USUALLY CONTACT VICTIMS VIA PHONE CALL

Those promising legitimate, part-time jobs tend to do so through messaging platforms such as WhatsApp or Telegram

Scam Type	*Email*	*Google Search*	*Messaging Platform*	*NA*	*Offline Channel*	*Other Apps*	*Phone*	*SMS*	*Social Media Platform*	*Website*
Bank Scam							75.00%		25.00%	
Fake e-commerce		25.00%							25.00%	50.00%
Impersonation Scam		9.09%	21.21%				51.52%		15.15%	3.03%
Investment			47.37%		5.26%	5.26%	15.79%		26.32%	
Legal Action		6.25%	18.75%	6.25%			62.50%	6.25%		
Miscellaneous		9.09%	9.09%	27.27%	9.09%	9.09%	9.09%	9.09%	18.18%	
Part time/Job Scam	4.55%		59.09%				18.18%		13.64%	4.55%
Tech/Customer Support		57.14%	14.29%				14.29%			14.29%

Table: Correlation of fraud type and initial access by perpetrators

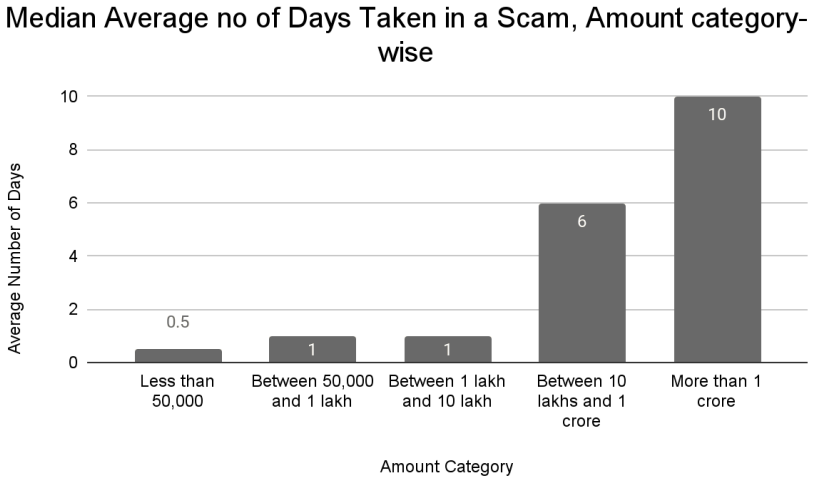
The point of initial contact varies across scam types, indicating certain points of initial access are more effective in certain kinds of scams e.g. phone calls for impersonation scams and messaging for investments.

DATA ANALYSIS

SCAMS ARE EXECUTED OVER MULTIPLE DAYS, ESPECIALLY WHEN FRAUD PERPETRATORS INTERACT WITH VICTIMS OVER PHONE CALLS

The communication channel plays a significant role in the duration of a scam, with phone call-based scams lasting longest, followed by Whatsapp-enabled ones.

Communication Channel	*Median Average of Duration*
Email	4
Facebook	0.5
Phone	12
Telegram	5.5
WhatsApp	9
SMS	0.5
Phone,SMS	2.5
Phone, Skype	1.5
Phone, Whatsapp	9
Whatsapp, Instagram	4
Whatsapp, Telegram	2
Whatsapp, Zoom	0.5



Communication is central to determining scam duration and impact, with longer interactions correlated with higher financial losses. Intervening in scam communication, particularly over phone calls where victims lack verification tools, can therefore significantly reduce scam amounts.

VULNERABILITY MAPPING

VULNERABILITY MAPPING

IN ADDITION TO THE LITERATURE REVIEW, EXPERT CONVERSATIONS REVEALED THE CENTRALITY OF VULNERABILITY IN FRAUD PERPETRATION

Alice E. Marwick highlights vulnerabilities across emotional, cognitive, and product levels in the global context

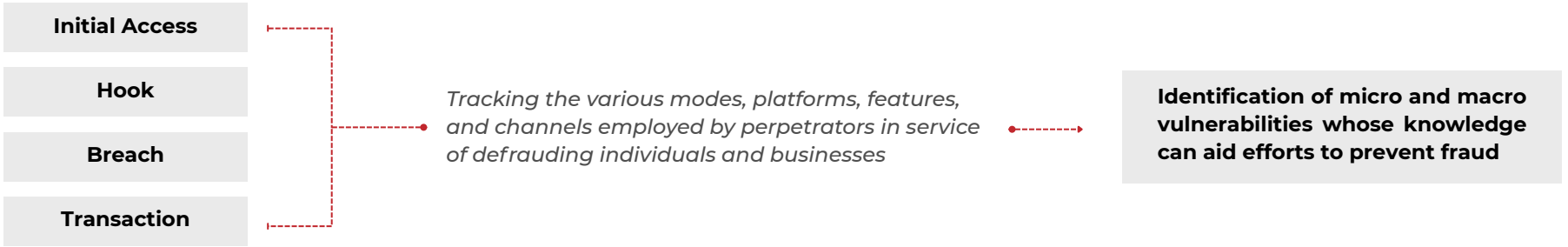
USER VULNERABILITIES	*PRODUCT VULNERABILITIES*
Scam susceptibility depends not only on technological literacy but also the exploitation of emotional triggers, especially around important stages in people's lives	Fraud perpetrators are increasingly incorporating AI into their MOs, exploiting the un-readiness of products to deal with AI-facilitated scams
Trust is exploited through personalization of the 'hook' and interpersonal cues	Newer ways of transacting have emerged in recent years e.g. crypto channels
The interconnectedness of 'grey area' products such as those of betting/gaming and scam culture presents difficulties	The lack of friction in user experience exposes product users to product/feature manipulation by fraud perpetrators

Although emotional vulnerabilities play a significant role in the success of fraud perpetration, product-level changes can accelerate user resilience.

VULNERABILITY MAPPING

INSIGHTS FROM THE FIR DATA POINT US TO SPECIFIC VULNERABILITIES THAT PERPETRATORS EXPLOIT ACROSS PEOPLE AND PRODUCTS

Perpetrators employ a host of techniques and digital tools, often leveraging them for novel use cases and across their interaction with the user from the time of initial access to the transaction

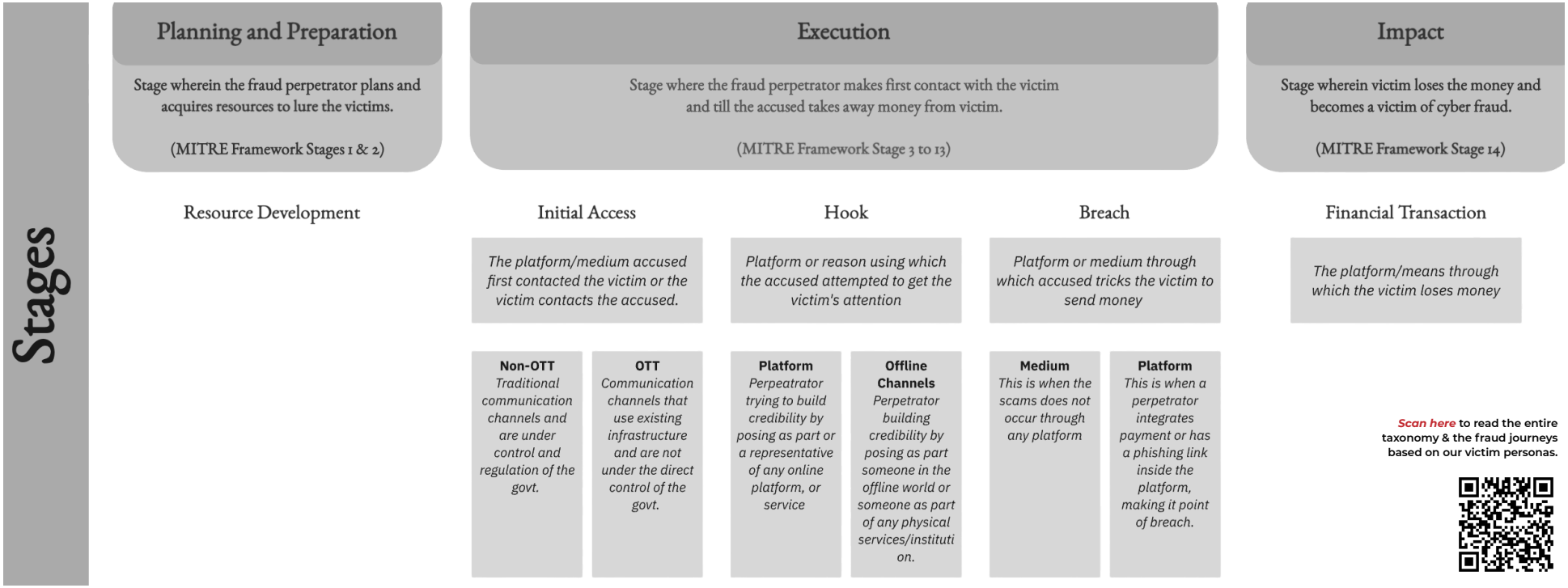


The point of initial contact varies across scam types, indicating certain points of initial access are more effective in certain kinds of scams e.g. phone calls for impersonation scams and messaging for investments.

VULNERABILITY MAPPING

BASED ON OUR ANALYSIS OF THE DATA, WE DISAGGREGATE AND TAXONOMISE VULNERABILITIES AT BOTH USER AND PRODUCT LEVELS

To understand how these vulnerabilities play out in victim-perpetrator interactions, it became essential to also examine the interplay between the various stages that comprise them

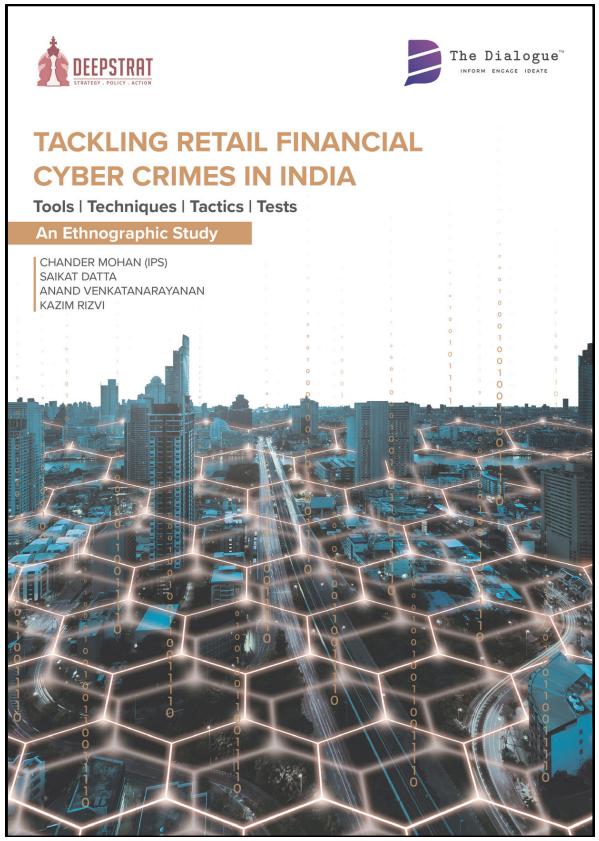


Scan here to read the entire taxonomy & the fraud journeys based on our victim personas.

This taxonomy is to be treated as a hypothesis, which we hope to test in future work.

VULNERABILITY MAPPING

SEVERAL VULNERABILITIES EMERGED IN DEEPSTRAT'S 2021 STUDY ON TACKLING CYBER CRIMES...



Vulnerabilities in Tackling Cyber Crimes

- There is no real-time data sharing among stakeholders (Police, Banks, Fintechs, etc)
- Need for dedicated and continuous studies on changing TTPs of fraudsters
- Capability to track payment transactions in real-time through regulatory mechanisms
- Lack of adequate product vulnerability awareness enabling fraudsters

...MANY OF THESE GAPS CONTINUE TO EXIST

USER VULNERABILITY

USER VULNERABILITY

IN THE CONTEXT OF FRAUD, WE THINK ABOUT VULNERABILITY IN A MULTIDIMENSIONAL SENSE

Both intrinsic and extrinsic factors contribute to the individual's vulnerability to becoming a fraud victim

REASONS TO TRUST

Factors that take precedence in the decision to give trust to the perpetrator or the platform

DEMOGRAPHIC CHARACTERISTICS

Individual characteristics such as age and financial status

EXPOSURE TYPE

The nature of the fraud that the individual is likely to fall for

The fraud victim personas are primarily based on the underlying emotional insecurity and cognitive bias that perpetrators target, moving away from a risk response framing to one foregrounding the risk itself.

USER VULNERABILITY

ANALYSING THE CONTENT OF FIRS HELPED IN THE DEVELOPMENT OF CODES FOR USER VULNERABILITY

These were further extended to build out personas of digital fraud victims, based on their needs, values, aspirations, and abilities

ANALYSE FIRs

"I initially made money doing part-time tasks, but to make big money I was told to invest."

"When I saw that money can be made easily, I was ready to invest."

BUILD CODES

Emotional vulnerability:
financial insecurity

Cognitive vulnerability:
confirmation bias, stranger trust bias

DEVELOP PERSONAS

The Aspiring Earner, Young, jobless, wants a job and quick money, believes that the internet can help fulfill this dream.

The Miro board also houses the victim persona cards and example journeys based on the taxonomisation of vulnerabilities.

Sources: SCARS Institute (2023, 2024)

PRODUCT VULNERABILITY

PRODUCT VULNERABILITY

PRODUCT VULNERABILITIES NEEDS TO BE UNDERSTOOD IN CONTEXT OF SCAMS TO DEVELOP MORE EFFECTIVE AND TARGETED SOLUTIONS

Exploitation of product vulnerabilities is not a matter of research hypothesis, but a persistent reality in the realm of online and digital products

> A product vulnerability is a *weakness, gap, or design flaw* in the features, user experience, or governance of a digital product/service that *can be exploited by malicious actors to defraud users*.

Real world examples

Scammers targeting a reward points system, exploiting server vulnerabilities, and leveraging weaknesses in API transactions for financial fraud

Exploiting vulnerability in the *wallet flow* of the payment service entity, targeting the integration between the payment service provider and merchants, to carry out multiple unauthorized transactions

Understanding and addressing vulnerabilities proactively could not only protect users, but also strengthen the resilience and credibility of the product in a competitive digital landscape.

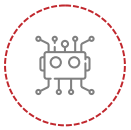
PRODUCT VULNERABILITY

VULNERABILITIES EMERGE DUE TO SHARED CHALLENGES ACROSS DIGITAL FINANCIAL PRODUCTS AND BUSINESS MODELS

Even when challenges appear product-specific, and how it is used by both users and perpetrators; they often recur across similar products and use cases.

Examples include:

Phygital dependency:
They rely on a mix of offline and online processes which creates leakages and gaps.



Partner/agent reliance:
They use intermediaries (agents, partner banks/NBFCs) which presents misrepresentation risk.

Slow/manual verification:
They take time (house verification, assignment forms). Fraudsters could exploit by promising "faster" alternatives.

Industry-wide spillover:
Fake apps and scams elsewhere hurt trust in legitimate fintech products.

We develop case studies around two applications - Communication and Payment - to diagnose their vulnerabilities from a fraud-specific lens and carve out lessons for other ecosystem players.

CASE STUDIES

CASE STUDIES

WE AUDITED USER JOURNEYS ACROSS A MESSAGING APPLICATION AND A DIGITAL PAYMENT PLATFORM

In this case study, *platform* refers to the digital application layer that enables user-to-user or user-to-business interactions and transactions within a bounded, feature-defined environment.

Mapped the user journey from registration and discoverability to communication, transactions, and grievance redressal.

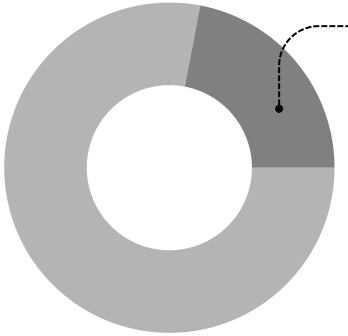
Examined how platform features and safety tools address or fail to address fraud-related risks.

Identified design gaps on the platform that enable impersonation, scams, and other fraudulent activity.

This exercise revealed how a product's design choices can either open doors to fraud or build layers of trust and safety for users.

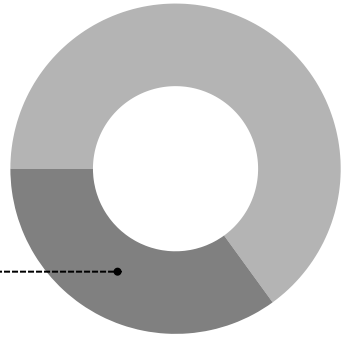
CASE STUDIES

DIGITAL COMMUNICATION PLATFORM XYZ* IS ENTRENCHED IN INDIA'S COMMUNICATION AND MARKET ECOSYSTEM



22% of FIRs mentioned digital communication platform as the platform where perpetrators *initially made contact* with victims

35% of FIRs mentioned digital communication platform as a mode of *communication* between perpetrator and victim



> Since it is the most popular ***messaging platform in India***, and is often used as a ***communication platform for facilitating fraud and contacting potential victims***.

"I was added to a group titled "--- Bank Secrets", and I saw many people were making money in it. That is when I contacted one of the members for investments."

This case study highlights how product design can expose users to fraud, but adding friction, trust-building features, and safety tools can reduce this exposure and equip them with the tools they need to protect themselves.

*A specific communication platform was reviewed to build out this case study, anonymised for the report.

CASE STUDIES

Discovery & Account Verification

WEAK VERIFICATION AND VISIBILITY CONTROLS ENABLE IMPERSONATION AND FRAUDULENT BUSINESS INTERACTIONS

Product feature or gap	*Impact on user vulnerability to fraud*
Lack of mandatory details or verification processes required for registering business accounts, such as date or year of registration	Does not provide users with sufficient information to verify business authenticity or legitimacy
Lack of additional verification requirements for certain business type: investment, or finance	Allows scamsters to operate in high-risk business categories to operate without due checks
Lack of friction or limits on changing usernames or switching between personal and business accounts	Makes it harder for users to verify authenticity as it becomes easier to hide one's identity, confuses users
Lack of user caution prompts for links received from unknown numbers or unverified businesses	Reduces user awareness and friction, leading to higher click-through rates on scam links

CASE STUDIES

Discovery & Account Verification

WEAK VERIFICATION AND VISIBILITY CONTROLS ENABLE IMPERSONATION AND FRAUDULENT BUSINESS INTERACTIONS

Product feature or gap	*Impact on user vulnerability to fraud*
Lack of mandatory details or verification processes required for registering business accounts, such as date or year of registration	Does not provide users with sufficient information to verify business authenticity or legitimacy
Lack of additional verification requirements for certain business type: investment, or finance	Allows scamsters to operate in high-risk business categories to operate without due checks
Lack of friction or limits on changing usernames or switching between personal and business accounts	Makes it harder for users to verify authenticity as it becomes easier to hide one's identity, confuses users
Lack of preventive measures to stop registration of accounts under the names of other businesses	Makes it harder for users to verify between fake and legitimate business accounts

CASE STUDIES

Communication

GAPS IN CONTROLS AND PRIVACY SETTINGS INCREASE EXPOSURE TO UNSOLICITED MESSAGES AND MALICIOUS LINKS

Product feature or gap	*Impact on user vulnerability to fraud*
No default privacy settings in the application to block or restrict voice and video calls from unknown users	Exposes users to unsolicited potential scam calls, increasing chances of engagement
Lack of default settings in the application to prevent automatic media downloads	Enables automatic downloads of malicious or fraudulent content, putting users at risk of data theft or device compromise
Lack of default settings in the application to prevent unknown numbers from adding users to groups	Allows bad actors to add users to groups without consent, exposing them to phishing links and fraudulent schemes
Lack of limits on the number of messages that can be sent to unknown accounts	Enables fraud perpetrators to send bulk or repetitive messages to unsuspecting users, increasing exposure to scam attempts
Lack of warnings or restrictions on sharing and downloading APK files	Allows users to unknowingly install malicious applications that can steal data, access personal information, or compromise device security

CASE STUDIES

Platform Communication & Grievance Redressal

LIMITED GRIEVANCE REDRESSAL AND REPORTING TRANSPARENCY WEAKEN USER TRUST AND REDUCE PLATFORM ACCOUNTABILITY

Product feature or gap	*Impact on user vulnerability to fraud*
Lack of mandatory grievance redressal details for registered business accounts based on their reach or size	Prevents users from easily identifying responsible parties or escalation channels, and enabling businesses to evade accountability
Lack of signaling or alerts for messages or users reported multiple times as fraudulent	Exposes users repeatedly to known scam accounts, increasing the likelihood of falling for repeated fraud attempts
Lack of an option and process to report specific fraudulent links and provide detailed reasons (for e.g.- cyber cell helpline) e.g.- Suspect Repository	Limits users' ability to flag link-based scams, allowing harmful content to circulate unchecked and reach more victims instead of reaching the cybercrime and alerting the platforms to act on credible evidence
Lack of transparency about reported user accounts	Prevents users from understanding action taken, lowering trust in the platform's safety systems and discouraging reporting

CASE STUDIES

Transaction

LIMITED SAFEGUARDS IN USER–BUSINESS INTERACTIONS EXPOSE USERS TO PAYMENT FRAUD AND DATA COMPROMISE

Product feature or gap	*Impact on user vulnerability to fraud*
Lack of information such as IFSC code to users when making payments to business accounts	Increases risk of users transferring money to fraudulent accounts without realizing, as they lack cues to verify
Lack of warnings or alerts for external payment links redirection after the user clicks on them	Leaves users unaware of potential phishing or fraudulent links disguised as payment requests

CASE STUDIES

HOWEVER,
PRODUCT VULNERABILITIES THAT CAN BE ADDRESSED THROUGH DESIGN AND SAFETY FEATURES

Silence calls from unknown callers

Shows details like the person that added you, when the group was created to help users decide whether to stay in a new group

Automatically muted notifications, detailed group information, and easy options to leave or report the group without opening the chat

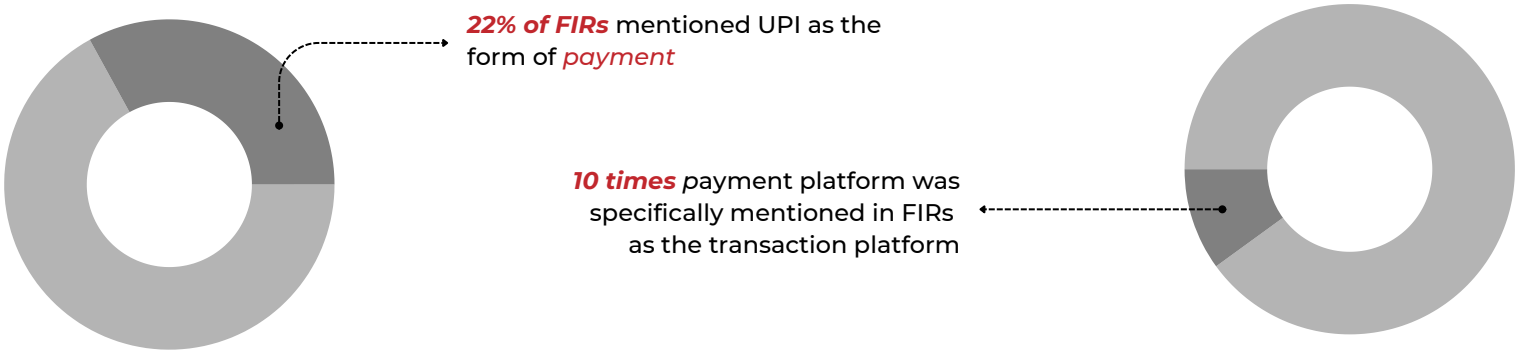
Links sent by unknown contacts remain inactive until the user responds, adds the sender to contacts, or manually copies and opens the link

These features and safeguards demonstrate how proactive, user-centered design can introduce meaningful friction in user interactions to strengthen trust and reduce fraud risks.

CASE STUDIES

OWING TO A WIDE USER BASE, FRAUD PERPETRATORS ALSO FREQUENTLY TURN TO DIGITAL PAYMENT APPS

It offers insights into how speed and frictionless payments can be weaponised by bad actors



> The ease of making payments using UPI and its large scale adoption makes it a popular choice amongst fraud perpetrators convincing victims to make payments.

"I received a call from someone claiming to be my dad's friend. He paid me some money, saying my dad had asked him to. Later called me and said 'Oh! Beta, check your message I accidentally paid you 25k, instead of 2.5k. Can you return the excess to me the?' I did not suspect fraud and paid him back."

The digital payment case study highlights how product design can expose users to scams, but adding friction, trust-building features, and safety tools can reduce this exposure.

*A specific communication platform was reviewed to build out this case study, anonymised for the report.

CASE STUDIES

Discovery & Account Verification

WEAK VERIFICATION ENABLES FRAUDSTERS TO IMPERSONATE ENTITIES, INITIATE CONTACT, AND SCALE FRAUDULENT OUTREACH

Product feature or gap	*Impact on user vulnerability to fraud*
Lack of search bar/verification process to identify authentic high-value businesses or financial institutions	Lack of verification, confuses users on legitimacy of a payment method
Lack of amount limit-based information sharing - Bank allows money transfers without displaying details on branch name or account type in high value transactions	Lack of information, denies users means to informed decision-making
Quick user login with only single OTP-based verification, which is inadequate	Provides ease in stealing data, further used for defrauding users
No limits on changing user profile details - including UPI ID, and profile pictures	Confuses victims with visual cues of authentic businesses/officials
Weak KYC mechanism for registration of business and lack of basic information such as business type	Confuses users with legitimate-sounding banking names such as “ABC Trading ”

CASE STUDIES

Communication | Platform Communication & Grievance Redressal

THE PAYMENT PLATFORM HAS WEAK DEFAULT PRIVACY SETTINGS AND REPORTING MECHANISMS

Product feature or gap	*Impact on user vulnerability to fraud*
Weak default setting allows users to use payment application with remote access and screen sharing (at certain stages)	Provides easy means for fraud perpetrators, exposing sensitive information and allowing control of bank accounts
No reporting mechanism inside the application for fraudulent transactions	Does not offer users an accessible and easy reporting procedure, helping perpetrators remain undetected
No reporting or flagging of suspected UPI IDs for fraud done by citizens	Leaves users unaware of suspicious accounts
Weak privacy setting that makes one's phone number the default UPI ID to be phone number (e.g. unlike Google Pay)	Exposing user phone numbers, enabling bad actors to build a database from legitimate transactions

CASE STUDIES

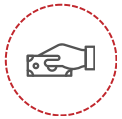
Transaction

THE PAYMENT PLATFORM ALLOWS LITTLE PAYMENT CONTROL TO ITS USERS

Product feature or gap	*Impact on user vulnerability to fraud*
Lack of ability to enter spending limits for UPI/wallets inside the application	Provides no friction for users, allowing perpetrators to exploit emotionally vulnerable victims taking quick decisions
Lack of behavior based notifications e.g., “You haven’t transacted with this user before. Proceed carefully.”	Does not give users slight cautious nudges, hindering informed decision-making
Lack of payment controls e.g. disabling payments from unknown or blocked users	Denies users control of their own bank accounts, allowing fraud perpetrators to initiate contact
Lack of flagging of suspicious payment patterns	Prevents users from insights to possible transactions with bad actors

CASE STUDIES

HOWEVER, THE PLATFORM PROVIDES CERTAIN FEATURES THAT EMPOWER USERS AND PROTECT THEM AGAINST FRAUD



Specific channels for paying certain financial institutions e.g. to pay loan EMIs

Prevents screenshotting of financial information that could be shared with bad actors

No payments to continue when screen sharing, in order to hide the UPI PIN

Notifies users on the primary device when a new device logs in and provides the option to log out of all devices

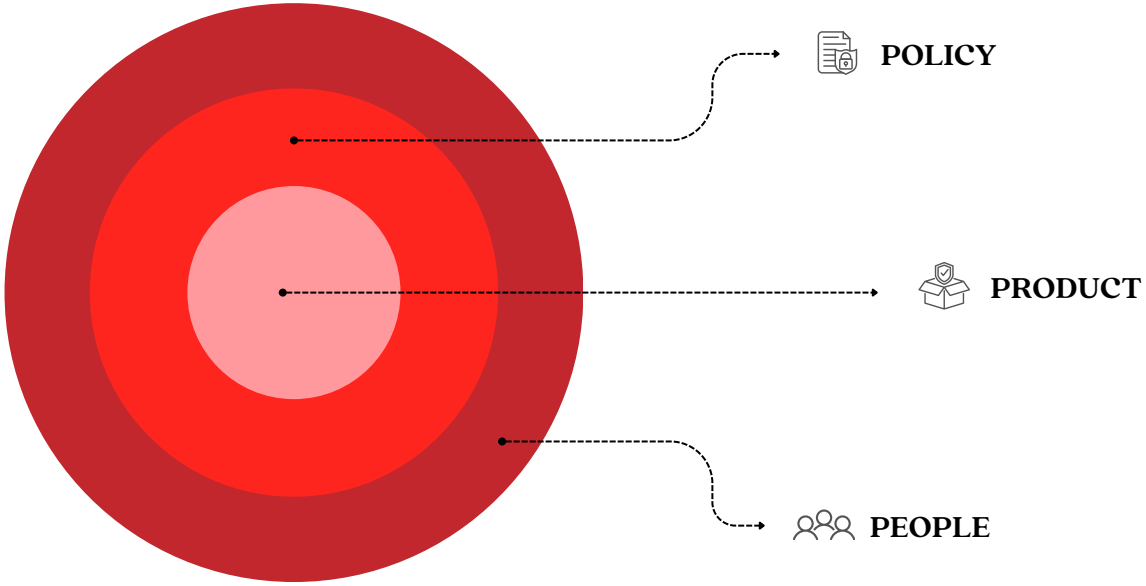
As a digital payments platform, it shows how minor nudges and providing necessary friction can help create a more scam-resilient platform, and it's absence can enable bad actors and fraudulent activity.

RECOMMENDATIONS

RECOMMENDATIONS

THE PEOPLE-POLICY-PRODUCT FRAMEWORK HELPS DISENTANGLE RECOMMENDATIONS

Recommendations at each level are supplemented with the nature of their impact - both on fraud perpetration directly, as well as on other spheres of influence



RECOMMENDATIONS

USER PROTECTION CAN BE SIGNIFICANTLY ENHANCED BY IMPROVING PRODUCT CONCEPTUALISATION AND DESIGN

Although it is the smallest of the circles, we find that these changes can have a small yet meaningful impact on policy considerations and user knowledge of harm prevention and response

01

Products should strengthen in-platform and app-store discoverability mechanisms to help users easily identify legitimate businesses and service (e.g.- Instagram, Line)

02

Contextual safety nudges for users within apps and communication platforms (e.g.- WhatsApp- This number isn't in your contacts)

03

Add "good friction" such as confirmation screens, time delays for high-value transactions, and alerts for risky behaviors such as first time payments.

04

Strengthen verification layers for businesses, sender identity checks, and visible trust markers. (e.g- grey tick for official government accounts)

RECOMMENDATIONS

ALTHOUGH REQUIRING BUY-IN, POLICY CHANGES PROVIDE SCOPE FOR SCALING UP RESILIENCE EFFORTS

As fraud tactics evolve, resilience requires coordinated shifts beyond user awareness and law enforcement responses

01

Shift from traditional post-fraud redressal mechanism by LEA's and banks to prevention-first measures (e.g., disallowing screen-sharing/ warnings by DBS & City Bank).

02

Encourage standardization of common design safety baselines for fintechs and platforms

03

Support longitudinal research and public data access on fraud trends to guide adaptive policy making. (e.g., ScamWatch by Australia).

04

Ensuring clear and shared responsibility for risks distributed across intermediaries such as banks, platforms, and payment aggregators. (e.g., Singapore's Shared Responsibility Framework)

05

Standardise domain name for services as a method of whitelist/verification - banks (bank.in), govt (gov.in) and potentially for financial institutions (fin.in) and create awareness on the standards

RECOMMENDATIONS

WITHOUT BURDENING INDIVIDUAL USERS, ENCOURAGING SOCIETAL RESILIENCE IS MOST IMPACTFUL

Building societal resilience against fraud requires shifting the focus from individual responsibility to collective systems of trust, empathy, and awareness

01

Run targeted awareness campaigns addressing emotional and cognitive vulnerabilities (e.g., authority anxiety) on platforms and existing regulation (e.g. TRAI's DLT regulations 2025 on SMS Suffix System to identify service, transaction, promotional and government msgs), rather than relying on generalized messaging.

02

Remove information asymmetry around loan and investment apps to ensure clearer discoverability of legitimate products through verified and official channels. (e.g., RBI's digital lending Guidelines).

03

Platforms, products, and public agencies should adopt non-blaming, empathetic messaging that encourages users to report scams

04

Provide victim-centric support to help individuals recover from the emotional and cognitive impacts of scam incidents. (e.g.- SCARS-Scam victim support and recovery)

WAY FORWARD

WAY FORWARD

THIS RESEARCH SETS INTO MOTION THE THEORY OF CHANGE FOR ECOSYSTEM RESILIENCE AGAINST FRAUD

A ‘theory of change’ delineates the path towards long-term resilience, against changing mechanisms of fraud perpetration

INPUT

A financial harms compendium and product diagnostics, to motivate long-term strategization

OUTPUT

Recommendations towards and testing of a digital resilience strategy for financial products

OUTCOME

Increased and long-term user trust in financial products

IMPACT

Sustained coordination between actors in service of a safe and resilient digital financial ecosystem

Analysing data from other jurisdictions, and testing the hypotheses built into the taxonomy bring us closer towards a long-term strategy.

WAY FORWARD

WHILE MANY PATHS FORK OUT OF THIS WORK, THE FOLLOWING MAY BE MOST USEFUL TO PURSUE

01

Cross-jurisdiction analyses of data pertaining to digital financial fraud for a pan-India knowledge system

02

In-depth co-design studios with IIMA Ventures portfolio start-ups for quick ecosystem impact

03

Study for a gender-intentional resilience strategy

04

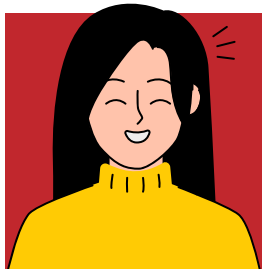
Study different financial service providers to develop specific and actionable interventions.

ANNEXURE

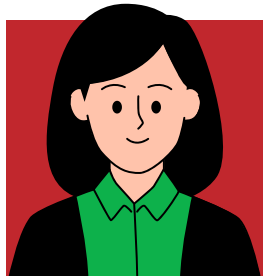
ANNEXURE

FOUR PERSONAS EMERGED IN AAPTI'S PREVIOUS WORK ON WOMEN'S DIGITAL TRUST

These were framed on the basis of user response to digital risk, a fundamental indicator of trust



The Learner
Risk - indulgent



The Native
Risk - informed

The Naysayer
Risk - minimallist

The Anxious
Risk - averse

The trust personas were subsequently imagined as a set of behaviours, not reflective of individual users.

ANNEXURE

THE TRUST PERSONAS OFFER A PATHWAY TO BUILDING FRAUD VICTIM PERSONAS

Although they cannot be imported as is, the larger persona framing organises our understanding of victim vulnerability by the circumstances and emotional insecurities of the victim. In doing so, it:

By identifying the socio-economic context and product level deficiencies, more suitable product-level design and policy-level interventions can be made, to create good friction and increased resilience for users.

Provides socio-economic context:

Perpetrators make use of underlying societal emotions that are deeply rooted in the social and economic context, and part of the popular psyche

Provides insight into limitations of existing products that enable fraud:

Persona mapping points to the specific areas where product design has been weak, thereby being unable to prevent, and sometimes even enabling, the defraudment of victims

ABOUT IIMA VENTURES

Built at IIM Ahmedabad in 2002 as an entrepreneurship centre and incorporated in 2007-08 as a section-8 company, IIMA Ventures (Formerly known as IIMA-CIIE) is the innovation continuum that studies, educates, incubates, accelerates, and invests in early-stage startups, aspiring entrepreneurs, and Investors.

IIMA Ventures has mentored over 10000 founders, accelerated over 2000 startups, provided catalytic capital to over 700 companies, and inspired over a million people with our 400+ publications. It has been a pioneer on multiple fronts including India's first accelerator - iAccelerator, India's largest idea scouting competition - The Power of Ideas, India's first climate fund - INFUSE Ventures, India's biggest platform for inclusive fintechs - Bharat Inclusion Initiative, India's first entrepreneurship bestseller - Stay Hungry Stay Foolish, Startup Compass and many more.

IIMA Ventures is recognised as a Centre of Excellence by the Department of Science and Technology, Government of India.

ABOUT DEEPSTRAT

DeepStrat is a think tank and strategic consultancy registered as a section 2 entity under India's Companies Act 2013. It combines the rich experience and expertise of its founders and strategic advisers in government and the private sector. DeepStrat and its partner organisations bring its network and experience in multiple sectors: Public Policy, Tax advisory, Cybersecurity, Technology, Project Design & Implementation, Risk Assessment & Management, Security, Foreign Policy. It has published research on a wide range of issues, while delivering customised and sustainable solutions for its clients on a range of issues ranging from policy, cybersecurity, taxation, risk management and technology solutions.

ABOUT AAPTI INSTITUTE

Aapti Institute is a Bengaluru-based research organisation which works at the intersection between technology and society to build solutions that enhance societal impact, justice and equity. Founded in 2018 by Sarayu Natarajan and Astha Kapoor, Aapti conducts research on emerging technology policy issues. Over the years, Aapti has worked with a number of partners globally on themes of data governance, digital inclusion, digital frauds, data stewardship, trust, data work and labour, gender and technology, climate-technology, migration-technology, information integrity, and responsible AI. Their work aims to empower policy development, particularly in the Global South, for an equitable and just digital world.

TAXONOMISING DIGITAL FINANCIAL FRAUDS FOR ECOSYSTEM RESILIENCE

If you'd like to know more about this work, please write to us at insights@iimaventures.com.

Access all our research at insights.iimaventures.com.

Digital Copy:

aapti institute

DEEPSTRAT
STRATEGY . POLICY . ACTION

Supported by IIMA VENTURES