Are Fraud-awareness Campaigns Effective?

Measuring the effectiveness of fraud-awareness campaigns and proposing recommendations for enhancing it.

Beni Chugh & Lakshay Narang

Executive Summary

Social engineering ploys, where unsuspecting customers are manipulated into authorising fraudulent transactions are a serious customer protection concern. Regulators and financial institutions are investing effort in designing awareness campaigns in the form of TV commercials (TVCs) to raise awareness about fraudsters and their tactics with the objective of reducing customers' tendency to engage with them. There is also a growing support for using outcome-based surveys (OBS) to test the effectiveness of such TVCs. Simple surveys that gather evidence on reported behaviour fall short of measuring effectiveness given that individuals depart from rational behaviour under the influence of behavioural biases. Consequently, OBS that gather evidence on change in behaviour are better suited to gauge the effectiveness of awareness campaigns.

This study presents the design of an OBS crafted to evaluate the effect that UPI-fraud-awareness campaigns have in reducing individuals' propensity to engage with fraudulent communication. Leaning on behavioral science and market research literature, this OBS measures the effectiveness of the awareness campaign along 4 dimensions: *recall,* i.e., the ability of the individual to remember the central message of the campaign, long after watching it, *appeal*, i.e., the extent to which individuals relate to the campaign, *comprehension,* i.e., the ease with which individuals understand the central message of the campaign and absorb it, finally, *impact,* i.e., a decline in individuals' tendency to engage with suspicious communication (messages, links, apps among others).

Insights from the OBS reveal respondents' preferences for TVCs with relatable characters and simple messages in a storytelling format. Such TVCs fare better on recall, appeal, and comprehension. The pilot also demonstrates that heightened awareness may not always translate into changed attitude. Awareness campaigns that solely emphasise conveying information or urging the public to improve their behaviour may disregard the inherent irrationality of human behaviour. Additionally, these campaigns often prioritise technical details about an issue rather than promoting self-awareness among their audience. To address this, awareness campaigns can be designed to acquaint viewers with their behavioural biases, which can make them vulnerable to social engineering tactics, thus fostering self-awareness. Moreover, these campaigns can provide guidance on avoiding or mitigating the impact of emotional states ('hot states'), which would positively influence the emotional aspect of attitudinal change and significantly enhance the effectiveness of the awareness campaigns.

I. Frauds appear to be a miniscule proportion of total UPI transactions but can have outsized effects on customers' confidence

UPI (Unified Payments Interface) is fast becoming embedded in the lives of customers. Reports suggest that UPI is dislodging other forms of digital and cash-based payments in urban areas while exhibiting strong growth rates in tier II cities and beyond (Press Trust of India, 2021). The Reserve Bank of India (RBI) reported a 1200% increase in UPI transactions in 2022 (Kaur, 2022). However, industry estimates suggest that the volume of UPI transactions grew by 500% in semi-urban and rural areas in the same period (LiveMint, 2022). The ease of making payments over chat, using QR codes and now offline through UPI Lite, appears set to add further momentum to the take-up of UPI even among the less savvy and newly banked customers.

A thorny customer protection issue that has been worrying both the regulators and the customers alike is the prevalence of frauds in UPI. The Ministry of Home Affairs (MHA), for instance, reported a 15% increase in fraudulent UPI transactions between the first and second quarters of 2022 (Kaur, 2022). For perspective, the reported number of fraudulent transactions is a very small proportion of the astronomical volume of payments realised over the UPI platform every month. For instance, 2021-22 accounted for about 74 billion UPI transactions while, per the numbers reported in the Parliament, the total number of fraudulent UPI transactions for the year stood at 95,000 (Das, 2023; Mudaliar, 2023).

Yet, the customer experience underneath the numbers reveals graver concerns. Dvara Research's primary research suggests that customers hesitate to report incidents of fraud due to a lack of faith in grievance redressal. The issue is more intricate in the case of women customers, who may hesitate to discuss incidents of fraud for fear of backlash or losing access to digital payments or even their smartphones. Beyond hesitating to report fraud, the study also suggests that a lack of trust in UPI is a prominent reason for its non-adoption, second only to the lack of access to a smartphone. In some instances, repeated fraudulent UPI transactions may completely dissuade customers from using the payment platform, leading them to revert to making transactions in cash (Chugh, Prasad, Palsule-Balsari, Roy, & Ali, 2023).

Given UPI's ever-expanding reach and its promise for digital financial inclusion, addressing the incidence of frauds in UPI and safeguarding customers from it are both business and policy concerns.

II. Safeguards against frauds: Ex-post measures are riddled with gaps, warranting greater emphasis on ex-ante measures in the short run

Fraudulent transactions are not unique to the UPI ecosystem. The RBI had earlier devised a *Limited Liability Framework* for unauthorised electronic banking transactions, with a view to protect customers from fraudulent digital transactions such as card cloning, etc. That framework explicitly applies to Scheduled Commercial Banks, Small Finance Banks, and Payments Banks. In that framework, liability is apportioned on the basis of the customers' role in facilitating fraudulent transactions. Where the customer has not authorised a transaction or not contributed to its authorisation, (such as in the case of a data breach at a bank that exposes customers' card details and facilitates unauthorised transactions), the framework mandates that the responsible regulated entity (i.e., the entity which issues the payment instrument) fully compensate the customer. However, in cases where the customer is at least partially responsible for the unauthorised transaction, (for instance, when they may have unwittingly shared their payment credentials leading to a fraudulent transaction), the framework absolves the regulated entity of any liability, completely apportioning full liability and therefore, the full loss to the customer (Reserve Bank of India, 2017).

An analysis of fraudulent transactions in UPI suggests that customers' authorisation is often needed for completing the fraudulent transactions. To this end, fraudsters typically employ social engineering tactics

to manipulate customers into sharing information such as their UPI-PIN or deceive them into clicking on collection requests that masquerade as 'payment links' or even download malware that can fetch similar sensitive information without the customers' active engagement (Reserve Bank of India, 2022; Shreya, 2023). Given this active (though misguided) role of the customers, fraudulent UPI transactions cannot be deemed as unauthorised per se, but they may be characterised as ***unintended transactions*** that arise from manipulating customer behaviour often under misleading pretexts and strong information asymmetry. It appears that the existing Limited Liability Framework does not cover such unintended transactions or offer recourse to the customer.

The gaps in ex-post safeguards against UPI frauds make ex-ante measures such as customer awareness programs increasingly critical, at least in the short run. Although the efficacy of customer awareness programs is often called into question, in the case of UPI transactions, they may be a necessary policy tool. By educating customers about the typical modus-operandi of fraudsters, behavioural biases that operate on the customers themselves, awareness campaigns could potentially reduce customers' propensity to fall for those tactics, authorise unintended transactions, and potentially reduce the incidence of UPI-related fraud.

The success of awareness campaigns in changing customers' attitudes towards UPI-related frauds depends on the effectiveness of these campaigns. It is not surprising, therefore, that the RBI prioritises the measurement and enhancement of their efficacy. The RBI in its Payment Vision 2025 notes:

> "*The scope of public awareness campaigns under the "RBI Says" tag shall be widened to cover different payment systems and their effectiveness shall be gauged through the outcomes of customer surveys*" (Department of Payment and Settlement Systems, 2022)

Taking a cue from the RBI's priorities, this brief sets out: (i) the design for an outcome-based survey to test the effectiveness of UPI-fraud-awareness campaigns; (ii) pilot this method with a small set of new-to-UPI customers in two tier I and II cities; and (iii) propose recommendations for improving the effectiveness of the campaigns and the system as a whole, based on the findings from the field.

III. Designing outcome-based surveys: Impact, i.e., the ability to employ awareness when faced by a fraudster appears to be the key outcome of interest.

Designing an outcome-based survey (OBS): An OBS identifies proxies or markers for the intended outcomes of a policy intervention. It then seeks to measure the effect of the policy intervention on those proxies (Institute of Museum and Library Services, n.d.). An outcome refers to an observable and/or measurable change in the status quo due to the policy intervention (Harding, 2014). In the current context, the awareness campaign is the policy intervention, and a decrease in people's propensity to engage with social engineering tactics that lead to UPI-related fraud is the outcome of interest.

Therefore, the objective of the current OBS is to assess the effectiveness of frauds-awareness campaigns in reducing customers' inclination to engage with fraudsters preying on UPI customers. We call this **'impact'** of the awareness campaign.

A framework for gauging effectiveness of awareness campaigns

Building on the literature on gauging the effectiveness of awareness campaigns from the domain of market research (Jaideep, n.d.) (Hall, 2002), and behaviour science, this study identifies the following markers that, when considered together, may signal the effectiveness of awareness campaigns:

- *The **recall** of the campaign among viewers:* the effectiveness of the campaign first and foremost depends on the ability of the viewers to recall i.e., re-access from memory the key message and/or

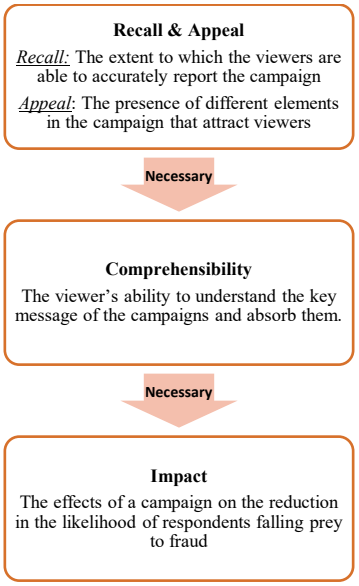
the elements of the campaign, even when noticeable time has lapsed since they were last exposed to the campaign (Jaideep, n.d.). The following sub-attributes contribute to making the campaign memorable:

  - ***Appeal*** *of a campaign closely aids recall*: It assesses the campaign's ability to connect with its target audience through elements such as the characters, the storyline, the emotions that get triggered by it, among others (Rajnerowicz, 2022). It leverages diverse emotions[1] to persuade viewers to act in a certain way.

- *Comprehensibility or the ability of the viewers to comprehend the campaign's message:* This indicator gauges if the central message of the campaign is effectively **comprehended** by the viewers (Jaideep, n.d.). Comprehension has two elements—the objective and the subjective. While recall and appeal influence objective comprehension, i.e., the ability to the viewer to understand the spoken message and written text of the advertisement; the subjective component is dependent on the viewers' ability to synthesise and absorb the message (IPL, n.d.). Therefore, there are aspects of comprehension beyond the influence of recall and appeal.
- ***Impact****, i.e., change in viewers' attitude towards fraudsters after viewing the ad:* It is a proxy for the change in the change in attitude of the viewers before and after viewing the campaign. This attribute examines if the campaign has a lasting impact on the viewers' behaviour in relation to the issue being targeted by the campaign. In summary, impact is a function of the other three attributes,

Figure 1: Framework for Assessing Effectiveness of Awareness Campaigns

The desired outcome (impact) of a campaign would depend on its ability to deliver information that is recallable, appealing, and comprehensible:



Shortlisting campaigns for gauging their effectiveness

[1] There are several types of appeals used in advertising such as emotional appeal, bandwagon appeal, scarcity appeal among others. In the campaigns of interest emotional appeal was the most leveraged type.

The RBI and the National Payments Corporation of India (NPCI) have implemented several campaigns over the years to educate customers about online fraud under their respective banners of "*RBI says*" and "*UPI Safety and Awareness Initiative*" (Reserve Bank of India, n.d.; National Payments Corporation of India , n.d.).

Among the campaigns introduced by the RBI and NPCI, a series of television commercials (TVCs) have also been created to raise awareness about UPI-related fraud. This study pilots the design of the OBS to assess the effectiveness of three TVCs: (i) the RBI's Security of Digital Transactions TVC, (ii) the RBI's Cyber Security TVC, and (iii) the NPCI's UPI Fraud Awareness AV. These TVCs are available in multiple languages.

The target audience

In this study, a sample of 80 respondents was selected from Delhi, Mumbai, Kolhapur (Maharashtra), and Unnao (UP). The choice of these cities was based on the assumption that residents in these areas (tier I and tier II cities) would be savvier than UPI users residing in tier III or tier IV cities. If the campaigns were found to be less effective in this savvier group, it would be reasonable to infer that their effectiveness among uninitiated individuals in remoter cities would potentially be even lower. The selection of respondents adhered to the following criteria: (a) an equal representation of genders; (b) new mobile internet users, who may have migrated online within the last 18 months; (c) new UPI users who may have started using the platform within the last 6-8 months; and (d) belonging to low-income households with an average monthly income between Rs. 15,000 - 25,000 and, (e) preferably engaged in migrant and/or gig economy work.

Applying the framework to design an OBS for assessing the effectiveness of fraud-awareness campaigns

Building on the theoretical intuition discussed earlier, the OBS seeks to gauge a change in the viewers' disposition to engage with attempted frauds. This is achieved through the following key stages of the study design:

- *Stage 1 - baselining awareness and disposition to attempted frauds:* This stage recorded customers' tendency to engage with frauds by exposing them to seven vignettes depicting common modus operandi of frauds. The researchers presented messages propagated by fraudsters over social media to the respondents and probed them on how an average user would respond to such messages. By subjecting the respondents to relatable scenarios and common fraudulent communication, the researchers aimed to recreate a (weaker) version of the 'hot state'[2] that respondents were likely to experience when exposed to social engineering ploys. These responses were recorded and treated as a baseline disposition towards attempted frauds. Subsequently, the respondents were presented short films (unrelated to the study's topic) interspersed with a clutter of TVCs from various brands, including the TVCs of interest, namely those from the RBI and the NPCI. The objective of this exercise was to recreate the environment in which individuals were most likely to encounter UPI-fraud-awareness TVCs, thereby providing a conducive setup to assess their appeal and comprehensibility. After presenting the visual content, the respondents were requested to narrate what they had observed. They were not specifically probed about the TVC of interest but were simply requested to summarise the visual content. The readiness and clarity with which the

[2] A hot state is defined as charged state of affectation or as a phase of intense emotional arousal which significantly alters the weights attached to longer term goals and nudges individuals towards short term decision making and impulsive behaviour (Reid, 2010).

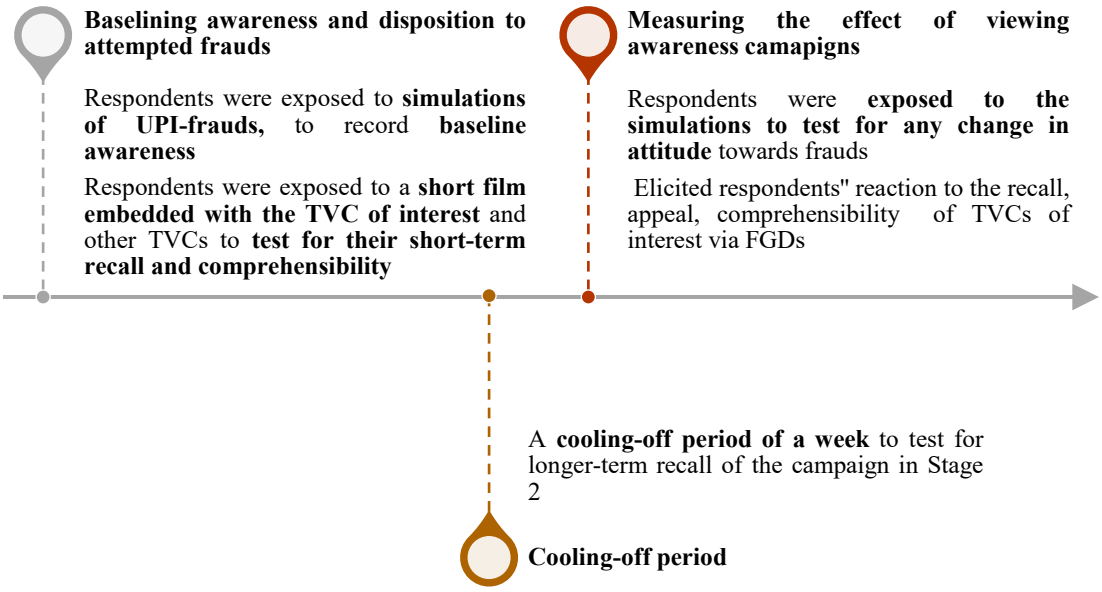
respondents were able to describe the TVC of interest served as markers of appeal and, to a lesser extent, short-term recall value of the TVC. TVCs and the video content were presented in relevant regional languages across each geography.

- *Stage 2 - measuring the effect of viewing the awareness campaigns:* The respondents were contacted after a week of the baselining exercise to gauge the effect of having viewed the awareness campaigns. Respondents were again presented with the same vignettes as in Stage 1 and were probed about what would an ideal response to the situation be. A favourable change in their response, i.e., a response signalling disengaging with the messages was treated as a weak but positive indicator of the effectiveness of the campaign. An adverse response, i.e., where respondents favoured engaging with the messages was treated as a (weak) marker of ineffectiveness of campaigns. This exercise allowed the researchers to comment on the 'impact' of frauds-awareness campaigns.

Post the vignettes, respondents were exposed to all three TVCs, independently. They were requested to summarise the TVCs and were probed about which TVCs were more preferred and why. This qualitative discussion in a focus group discussion (FGD) set-up allowed the researchers to form an impression of the comprehensibility and appeal of the TVCs.

The seven-day interval between the two stages is a crucial element of the study. This cooling-off period of sorts allows to test for recall value of the study. The danger in placing the two stages too close to each other is that the message could be fresh in the respondents' memory, therefore, priming them for responding favourably in the second stage.

Figure 2: Stages of the pilot



IV. Discussion: Awareness about frauds insufficient to bring about a behavioural change

Respondents' reaction to TVCs: What resonated with them

As discussed before, the study assessed the effectiveness of three TVCs: (i) the RBI's Security of Digital Transactions TVC; (ii) the RBI's Cyber Security TVC; and (iii) the NPCI's UPI Fraud Awareness AV. All three TVCs used different formats to disseminate information pertaining to UPI-related fraud. For instance, the RBI's Security of Digital Transactions TVC used a conversational format while the RBI's Cyber Security TVC adopted a monologue approach and included a famous Indian actor. The NPCI's Fraud Awareness TVC on the other hand, disseminated rich and detailed information through animation. Respondents reacted differently to each:

Recall: As mentioned in section III, recall of a TVC is a function of its appeal (to a lesser extent comprehensibility). For example, the use of a catchy and simple tagline, such as "no sharing", significantly enhances the comprehensibility and, in turn, the recall value of a TVC. Similarly, TVCs that feature conversations between characters in relatable and commonplace situations tend to leave a lasting impression, helping viewers remember the TVC.

Appeal: Individuals find TVCs with a conversational format between relatable characters in an ordinary setting more appealing than those with a monologue or animation. The appeal of a TVC is further enhanced if it includes a popular celebrity. Conversely, TVCs that overload viewers with excessive information tend to have lower appeal, and, in turn, recall. This is especially true when the format of the advertisement is closer to a monologue as opposed to a conversation.

Comprehensibility: Comprehensibility is enhanced when TVCs provide concise and unambiguous information. For example, the tagline "no sharing" effectively conveys the primary message of the TVC,

which is to refrain from sharing OTPs and PINs with others. Similarly, the inclusion of a well-known celebrity can assist in effectively conveying the TVC's message to viewers. While these affect the objective dimension of comprehension, the posture of the celebrity in the advertisement affects the subjective dimension of comprehension. For instance, viewers make note of and aspire to replicate the calmness with which a celebrity is shown to conduct themselves in the face of a fraud.

Impact: The study did not find a consistent pattern in the way the respondents' tendency to engage with attempted frauds changed after being exposed to the awareness campaigns. Of the seven vignettes, respondents reported a decreased tendency to engage with fraudsters in only three instances. In three other instances, respondents reported a higher inclination to respond to misleading communication than what they reported before viewing the awareness campaign. Both— the exposure to awareness campaigns and a high foundational awareness around frauds[3] did not readily translate into heightened hesitation in engaging with such communication. The subsequent sub-section explores potential reasons for this inconsistent behaviour.

Awareness campaigns, though necessary, may be inadequate to overcome behavioural biases

It would be naïve to assume that greater awareness would automatically translate into altered or improved behaviour. It is now well understood that mental biases and other predispositions prevent people from acting rationally and in their best interest. The study uncovered similar drivers behind peoples' tendency to engage with fraudulent communication.

The two dominant categories of factors that contribute to this vulnerability, namely intrinsic factors, and situational factors, as highlighted by Wen et al. in 2022 (Wen, et al., 2022). The intrinsic factors exist regardless of the context of the fraudulent transactions and are inhering personality traits or world views of the victim. They include psychological traits such as risk aversion, being open to trusting, among others, and, perceptions cemented through past experiences of digital transactions, encounters with fraudsters as well as motivations such as greed and fear (Langenderfer & Shimp, 2001) The situational factors are reinforced during the scam process. These factors encompass emotional imbalance, manifested by a heightened state of affectation or a 'hot-state', as well as cognitive biases which lead victims to defer decision making to heuristics and ignore the red flags in the environment (Wen, et al., 2022).

When individuals engage in fraudulent interactions, a combination of intrinsic and situational factors come into play, thereby activating various behavioural biases and rendering them more susceptible to falling victim to fraud. This study specifically finds the presence of intrinsic and situational factors that contribute to this susceptibility, which include:

- *Intrinsic factors*:

Personality traits[4]: Traits such as a tendency to take and undermine risks or trust familiar brands influence how individuals perceive and respond to fraudulent communication. For example, individuals who are generally more trusting may be more inclined to trust the contents of a suspicious message and ignore markers of fraud. Similarly, individuals who inaccurately perceive risk emanating from a suspicious message offering a small reward, may be more likely to engage with it.

[3] Most respondents reported receiving fraudulent calls/text messages and nearly half of the respondents reported that their close network had also received such communication. Similarly, a significant number of respondents reported having viewed UPI fraud awareness communication including the TVCs of interest in some instances.

[4] Wen, X., Xu, L., Wang, J., Gao, Y., Shi, J., Zhao, K., . . . Qian, X. (2022). Mental States: A Key Point in Scam Compliance and Warning Compliance in Real Life. *Int J Environ Res Public Health*.

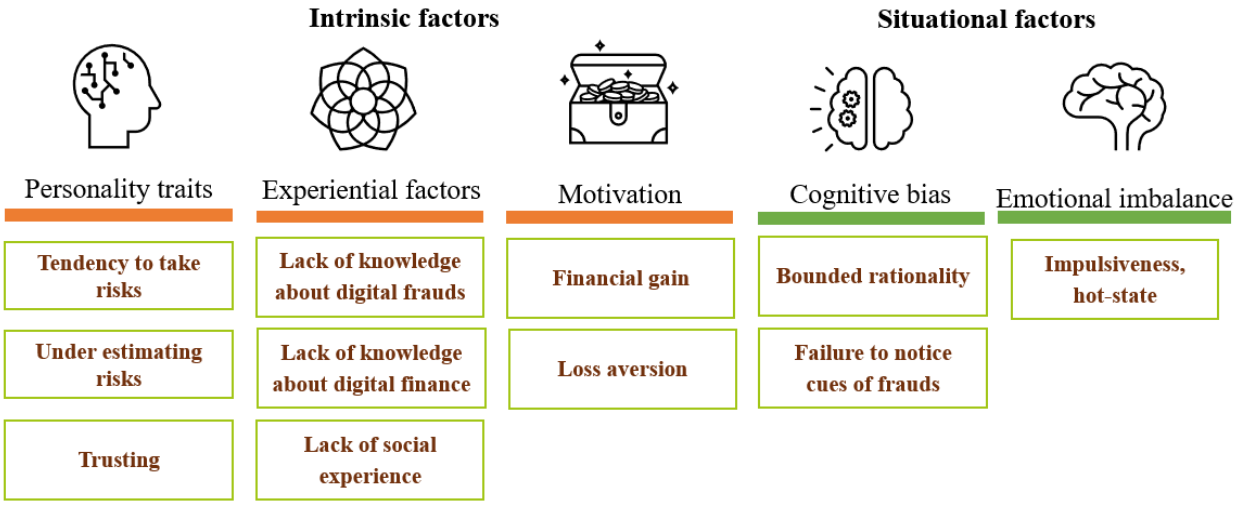
Experience factors: Factors such as a lack of knowledge about digital financial services or limited experience with them can undermine individuals' confidence in their understanding of the system, thereby making them more vulnerable to fraud. For example, respondents who had been defrauded in the past were reluctant to engage with any communication they received.

Motivation[5]: It plays a pivotal role in shaping individuals' propensity to engage with suspicious communication. This motivation is driven by visceral factors, namely greed and fear, which fraudsters frequently exploit. These factors manifest as a strong desire for financial gain or a fear of potential loss (Langenderfer & Shimp, 2001). For instance, individuals who are primarily motivated by financial gain are more prone to taking risks and responding to dubious messages that promise lucrative rewards. Conversely, those motivated by loss aversion are more inclined to dismiss suspicious messages in order to safeguard their financial resources. However, it is crucial to note that the fear of monetary loss can serve as a compelling motivator, leading individuals to allocate their cognitive resources towards preventing such losses and disregarding cues that may indicate fraudulent activity (Langenderfer & Shimp, 2001).

- *Situational factors*:

Cognitive biases[6]: Such biases are triggered by fraudsters in the process of fraud. Fraudsters often employ techniques that create a sense of urgency, pressuring individuals to make hasty decisions in an emotionally distressing state. In such circumstances, people tend to rely on heuristics, acting impulsively and overlooking warning signs. Individuals with limited knowledge or experience with digital financial services may be more vulnerable to these techniques and may struggle to identify fraudulent communication.

Figure 3: Customer's behavioural biases



Source: (Wen, et al., 2022). *Visualisation: Author's own*

Uncovering these biases provides two important lessons for policymakers aiming to reduce the occurrence of frauds in UPI and other contexts.

Firstly, relying solely on awareness campaigns may prove insufficient for inducing behavioural change. Awareness campaigns that solely focus on providing information or urging the public to behave better may

[5] Ibid
[6] Ibid

overlook the inherent irrationality of human behaviour. Such campaigns run the risk of oversimplifying the problem as a mere ***lack of information*** and assume that rational individuals, when adequately informed, will adjust their behaviour accordingly (Nurzhynska, 2020; Hauser, 2022). However, the biases discussed earlier highlight the limitations of such an assumption. Therefore, while necessary, increased awareness alone may not always translate into significant changes in behaviour (Christiano & Neimand, 2017).

Furthermore, behavioural science indicates that an individual's attitude comprises three dimensions: cognitive (related to knowledge levels), affective (related to emotional makeup), and behavioural (informed by both cognitive and affective aspects) (Scandura, n.d.; Nurzhynska, 2020). Thus, individuals' knowledge or information levels only partially influence their attitudes. In the present context, it appears that the awareness campaigns examined in this pilot disproportionately leverage the cognitive dimension. While the campaigns evoke emotions among viewers, a type of appeal called emotional appeal, they do not necessarily cause users to become self-aware of the emotional state that the fraudsters are looking to evoke in them. A lack of attention to this aspect of affective dimension in this regard misses on highlighting for viewers the emotionally charged state or 'hot-state' that they are likely to experience and how that forces them to comply with the demands of the fraudster. Perhaps familiarising users to the hot state and guiding them on overcoming it could make the campaigns more effective. A more detailed discussion on this topic is presented in Section V.

Secondly, even the most effective awareness campaigns will remain insufficient in reducing the occurrence of frauds. Behavioral change must be accompanied by structural safeguards that deter customers from falling for frauds and provide expedited recourse in the event of financial losses to fraudsters. Some potential areas for structural reforms are briefly discussed in the concluding section VI.

V. Enhancing the effectiveness of awareness campaigns: Complementing awareness with self-awareness

Incorporating behavioural biases while designing TVCs may affect attitudinal change:

As discussed earlier in section IV, attitudinal change requires addressing both the cognitive and affective dimensions. The awareness campaigns studied in the pilot risk underestimating the affective dimension. Affective awareness may help individuals overcome behavioural biases and the emotional imbalance that influence them when they encounter social engineering tactics. Campaigns that alert individuals to their own adverse behavioural loops and provide guidance on how to break free from them may hold the promise of driving behavioural change. The *Take Five* initiative in the UK serves as a good example of such a campaign. The campaign recognises that customers fall victim to scams not due to lack of awareness but because they struggle to apply that awareness when overcome by their 'hot state'. Therefore, the campaign emphasises strategies that assist customers in identifying the 'hot-state' and, consequently, managing the affective challenges by (i) pausing and reflecting before complying with fraudsters to dissipate their 'hot state'; (ii) challenging themselves to ensure they are not being defrauded; and (iii) protecting themselves by reaching out to their bank and authorities in case of fraud (Take Five to Stop Fraud, n.d.). Another example is the fraud awareness campaign conducted by the Federal Trade Commission (FTC), one of the customer protection agencies in the USA. In their campaign, the FTC educates customers about typical tactics used by scammers, such as promising rewards or creating urgency for immediate action. However, the campaign goes beyond mere awareness by reminding viewers of useful tips to avoid being governed by their biases. These reminders include pausing and refraining from immediate action and seeking advice from trusted individuals or authorities (Federal Trade Commission, 2022).

In a similar vein, awareness campaigns on frauds can emphasise typical behavioural vulnerabilities and help viewers become aware of their behavioral biases and foster self-awareness. The study revealed that

respondents were more likely to trust suspicious communication and engage with it if they believed it originated from a trusted source, such as financial institutions or renowned departmental stores. Respondents tended to trust such communication even without verifiable evidence confirming its legitimacy. Awareness campaigns should aim to cultivate a sense of skepticism among customers when interacting with unknown or suspicious communication. Further, when faced with doubts about suspicious communication, respondents often relied on their friends and family to verify its authenticity. This indicates that customers sporadically employed informal measures to validate suspicious communication. Awareness campaigns may tap into this desirable behaviour and remind viewers to confer with someone they think would know better before complying with a stranger.

More broadly campaigns could emphasise practices such as critical inquiry and requesting relevant and official documents, and information before making any payments.

VI. Going beyond awareness: Improving and complimenting the awareness campaigns

Responding to customer's needs: Providing end-to-end information to the customers

Incorporating information on post-fraud recourse:

The study uncovered a deep lack of awareness around what customers were supposed to do if they lost money to a fraud. Most respondents reported not knowing of the formal recourse channels and many reported they would approach peers to understand next steps. The TVCs of interest emphasise informing the viewer of how fraudsters may manipulate them. However, little attention is paid to explaining the actions that customers may undertake *after* they have lost money to a fraud. For instance, the RBI operates a helpline (14440) that provides comprehensive information on post-fraud remedies (Reserve Bank of India, n.d.) yet few respondents knew of it. It was also not emphasised in any of the campaigns of interest. Post-fraud recourse may become a central theme of future campaigns. Further, displaying information about recourse helplines may become a permanent feature of other UPI-awareness campaigns and other communication initiatives of the regulators such as SMSs from the RBI.

Structural safeguards can afford systematic protection from frauds

As mentioned previously, ex-ante measures like awareness campaigns alone may be insufficient to effectively mitigate the occurrence of fraud in UPI. While behavioural change is an important component, it is just one tool in the arsenal for protecting customers against UPI-related frauds. The advancement of technology has led to increasingly sophisticated fraud techniques. Therefore, a comprehensive approach to customer protection requires structural safeguards that encompass fraud detection, prevention, and investigation.

In this regard, we propose the implementation of several safeguards that can be integrated into or leveraged from the existing UPI ecosystem.

Firstly, simplifying the process for registering complaints related to UPI frauds is crucial. Currently, there appear to be parallel initiatives being operated by different regulatory and government departments such as that of the RBI, the Ministry of Home Affairs (MHA), in addition to reporting channels hosted by banks and even Third-Party Apps (TPAPs) in UPI. Providing a simplified and potentially unified reporting channel would facilitate prompt reporting from the customer.

Secondly, it appears that while several channels exist for reporting the loss of money, venues where customers can report attempted UPI frauds appear limited. Providing accessible and customer-friendly platforms for reporting suspicious incidents, even where customer may not have lost money would help

generate system-level intelligence about suspicious activity, enhancing the effectiveness of fraud prevention efforts.

Thirdly, establishing a system-wide fraud registry by expanding the scope of existing information systems and integrating them would be beneficial. This registry could serve as a centralised repository of fraud-related data, enabling efficient information sharing and analysis across various stakeholders. It could also double up as an enforcement tool, designed to take or coordinate actions against suspicious or fraudulent activity, basis pre-determined protocols.

Lastly, developing a solution that assists customers in distinguishing genuine callers from fraudsters is imperative. This could involve implementing caller identification mechanisms or providing guidelines to help customers verify the authenticity of incoming calls.

These safeguards are useful, system-level complements to behaviour change tools. Future research may focus on developing these safeguards to the satisfaction of all stakeholders to address the thorny issues of frauds in UPI but also digital finance.

References

Christiano, A., & Neimand, A. (2017). *Stop Raising Awareness Already*. Retrieved from Standford Social Innovation Review Web site: https://ssir.org/articles/entry/stop_raising_awareness_already

Chugh, B., Prasad, S., Palsule-Balsari, S., Roy, P., & Ali, S. A. (2023). *Making UPI Count: Making UPI payments more user centric for new-to-UPI users.* Dvara Research.

Das, B. (2023, April 19). *UPI dominated digital transactions in 2022, payments worth Rs 126 lakh crore recorded, says report*. Retrieved from Business Today Web site: https://www.businesstoday.in/industry/banks/story/upi-dominated-digital-transactions-in-2022-payments-worth-rs-126-lakh-crore-recorded-says-report-377991-2023-04-19#:~:text=Unified%20Payments%20Interface%20(UPI)%2C,per%20cent%20increase%20in%20value

Deepstrat; The Dialogue. (2022). *Tacling Retail Financial Cyber Crimes in India.* Delhi.

Department of Payment and Settlement Systems. (2022). *Payments Vision 2025.* Reserve Bank of India .

Federal Trade Commission. (2022, July). *How To Avoid a Scam.* Retrieved from Federal Trade Commission Consumer Advice Web site: https://consumer.ftc.gov/system/files?file=consumer_ftc_gov/pdf/1009a_how_to_avoid_a_scam_aug2022_508.pdf

Hall, B. F. (2002). A New Model For Measuring Advertising Effectiveness. *Journal of Advertising Research*, Vol. 42, No. 2.

Harding, A. (2014, October 27). *What is the difference between an impact and an outcome? Impact is the longer term effect of an outcome.* Retrieved from LSE Blogs Web site: https://blogs.lse.ac.uk/impactofsocialsciences/2014/10/27/impact-vs-outcome-harding/

Hauser, M. (2022, January 21). *Behavioural Science in action*. Retrieved from Esomar Web site: https://esomar.org/newsroom/behavioural-science-in-action

Institute of Museum and Library Services. (n.d.). *Home: Outcome Based Evaluations Basics*. Retrieved from Institute of Museum and Library Services Web site: https://www.imls.gov/grants/outcome-based-evaluation/basics

IPL. (n.d.). *The Importance Of Comprehension In Advertising*. Retrieved from IPL Web site: https://www.ipl.org/essay/Objective-Comprehension-In-Advertising-PJYLRAN2SG#:~:text=One%20is%20the%20Subjective%20and,message%20delivered%20by%20the%20advertiser

Jaideep, S. (n.d.). *Techniques to Measure Advertising Effectiveness*. Retrieved from Youth Article Library Web site: https://www.yourarticlelibrary.com/advertising/techniques-to-measure-advertising-effectiveness/48670

Kaur, J. (2022, November 14). *News: 1.4 Lakh UPI Frauds Reported In Q1, Q2 2022: MHA*. Retrieved from Inc42 Web site: https://inc42.com/buzz/1-4-lakh-upi-frauds-reported-in-q1-q2-2022-mha/

Langenderfer, J., & Shimp, T. A. (2001). Consumer Vulnerability to Scams, Swindles, and Fraud: A New Theory of Visceral Influences on Persuasion. *Psychology & Marketing*, Vol. 18(7): 763–783.

LiveMint. (2022, December 06). *UPI transactions surge 650% in semi-urban, rural stores: PayNearby*. Retrieved from Live Mint Web site: https://www.livemint.com/money/personal-finance/upi-transactions-surge-650-in-semi-urban-rural-stores-paynearby-11670311587769.html

Mudaliar, S. (2023, March 23). *Over 95,000 UPI fraud cases reported in 2022-23: Centre in Parliament*. Retrieved from Hindustan Times Web site: https://www.hindustantimes.com/india-news/over-95-000-upi-fraud-cases-reported-in-2022-23-centre-in-parliament-101679541121388.html

National Payments Corporation of India . (n.d.). *Home: An Awareness initiative by NPCI to educate users about the types of frauds which can happen and how one can easily avoid these frauds on UPI.* Retrieved from NPCI Web site: https://www.npci.org.in/upi-frauds-awareness

Newsroom Staff. (2022, February 17). *1930 is the new Helpline number against cyber crimes; netizens share their 'experience'*. Retrieved from Newsroom Post Web site: https://newsroompost.com/india/1930-is-the-new-helpline-number-against-cyber-crimes-netizens-share-their-experience/5066166.html

Nurzhynska, A. (2020, June 04). *Why should we change our approach to public campaigns?* Retrieved from LSE Web site: https://blogs.lse.ac.uk/psychologylse/2020/06/04/why-should-we-change-our-approach-to-public-campaigns/

Outlook Money. (2022, December 28). *RBI To Migrate Payments Fraud Reporting Module To DAKSH From Jan 1, 2023.* Retrieved from Outlook India Web site: https://www.outlookindia.com/business/rbi-to-migrate-payments-fraud-reporting-module-to-daksh-from-jan-1-2023-news-248936

Press Trust of India. (2021, January 12). *Online transactions grew 80% in 2020 driven by tier 2, 3 cities: Razorpay*. Retrieved from Business Standard Web site: https://www.business-standard.com/article/economy-policy/online-transactions-grew-80-in-2020-driven-by-tier-2-3-cities-razorpay-121011201085_1.html

Rajnerowicz, K. (2022, August 17). *Blog: 9 Types of Advertising Appeals That Actually Work*. Retrieved from Tidio Web site: https://www.tidio.com/blog/advertising-appeals/

Reid, A. (2010, December 07). *HOT-STATE DECISION MAKING: UNDERSTANDING CONSUMER EMOTION AND RATIONALITY.* Retrieved May 2023, from Sentinent Decision Science: https://www.sentientdecisionscience.com/hot-state-decision-making-understanding-consumer-emotion-and-rationality/

Reserve Bank of India . (2022, December 26). *Central Payments Fraud Information Registry – Migration of Reporting to DAKSH.* Retrieved from Reserve Bank of India Web site: https://m.rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=12431

Reserve Bank of India. (2017, July 06). *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions.* Retrieved from Reserve Bank of India Web site: https://rbi.org.in/Scripts/BS_CircularIndexDisplay.aspx?Id=11040

Reserve Bank of India. (2022). *Be(a)ware: A Booklet on Modus Operandi of Financial Fraudsters.* Reserve Bank of India. Retrieved from https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf

Reserve Bank of India. (2022, October 06). *RBI launches (DAKSH) - Reserve Bank's Advanced Supervisory Monitoring System.* Retrieved from Reserve Bank of India Web site: https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR10044753171E2C7D4DFA83186B72753421FF.PDF

Reserve Bank of India. (n.d.). *Home: Customer Liability in Unauthorised Transactions*. Retrieved from Reserve Bank of India Web site: https://www.rbi.org.in/commonperson/English/Scripts/SMSLimitedliability.aspx

Reserve Bank of India. (n.d.). *RBI Kehta Hai: A Public Awareness Initiative of the RBI*. Retrieved from RBI Kehta Hai Web site: https://rbikehtahai.rbi.org.in/

Scandura, T. A. (n.d.). *Essentials of Organizational Behavior: An Evidence-Based Approach*. Retrieved from SAGE Edge Web site: https://edge.sagepub.com/node/23655/student-resources/chapter-4/learning-objectives

Shreya, R. (2023, April 12). *The Use of Malware in UPI related Fraud*. Retrieved from Dvara Research Web site: https://www.dvara.com/research/blog/2023/04/12/the-use-of-malware-in-upi-related-fraud/

Take Five to Stop Fraud. (n.d.). *About Us: Take Five to Stop Fraud*. Retrieved from Take Five to Stop Fraud Web site: https://www.takefive-stopfraud.org.uk/about/take-five/

Wen, X., Xu, L., Wang, J., Gao, Y., Shi, J., Zhao, K., . . . Qian, X. (2022). Mental States: A Key Point in Scam Compliance and Warning Compliance in Real Life. *Int J Environ Res Public Health*.

What is Action Fraud?: . (n.d.). Retrieved from Action Fraud Web site: https://www.actionfraud.police.uk/what-is-action-fraud

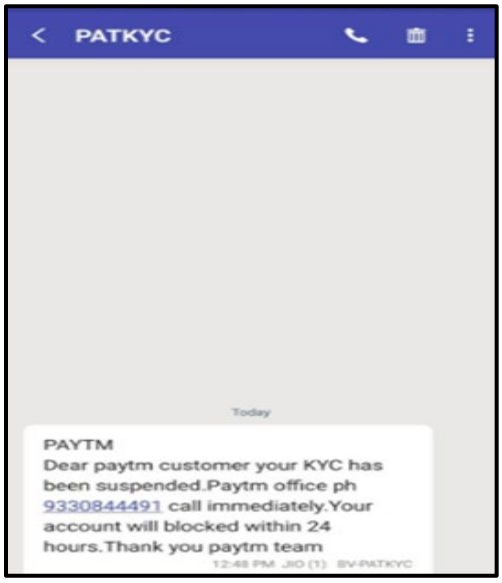
Appendix-1

Simulations of frauds presented to the respondents

The fraudulent communications chosen for the study:

i. I am calling from your bank. It appears there has been a fraud on your Debit card and some money has also been deducted. I am calling to help you, but before we proceed, can I have some details for verification? I will need your full name, debit card number and PIN
ii. Pravin/ Shikha's husband/wife works in the city and wants to send her some money. He asks for her UPI id, but she doesn't know how to give it to him. She sees her local shopkeeper and asks him to help her. She unlocks her phone and gives it to him
iii. Congratulations! You've won a lucky draw for Rs 10,000/-. The money is ready to be transferred to your account. We have sent a 'Collect' request to your UPI id. Once you click on the Collect button, the money will be credited to your account
iv. Madam, I am calling from D Mart/Apna Bazaar. We have received export quality mangoes which we are selling to some of our special customers for Rs. 400 per dozen. Please make payment to this number: 98201555405 and we will deliver the mangoes to you in an hour
v. Congratulations Ma'am! You have won a lottery of Rs. 10,000. Please let me know your UPI id and PIN so that I can transfer the money.

Additionally, the study employed the following two visual cues of suspicious messages:



Source: Suspicious communication received by the team and reported in the media.