MSC Policy brief #28

Decoding the extent and exposure of financial fraud among DFS customers

Arshi Aadil, Gayatri Ahuja, Ritika Sah, and Shrutkirti Dhumal

MSC
MicroSave Consulting

Research team

Gayatri Ahuja

Lakshay Jain

Ritika Sah and

Shrutkirti Dhumal

Review Support

Graham A.N. Wright and

Jenifer Shapiro

Introduction and background

A momentous shift is unfolding amid the rapid transformations that have swept through India's economic landscape. The country is in transition from a cash-based economy to a dynamic digital space that has ushered in newfound financial inclusion for population segments that have been so far marginalized.

Since 2018, financial inclusion in India has improved at a CAGR of 5%, while the transaction value in digital payments stood at USD 44 billion in the second quarter of 2022. India has seen digital financial services (DFS)-related fraud rise amid an increase in the use of formal financial services and the reliance on digital rails, such as UPI (Unified Payment Interface). Fraud in DFS has risen from USD 18.8 million reported in 2022 through cards and internet banking to USD 33.6 million in FY23.

However, notably, 94.5% of the reported fraud cases in 2023 occurred in previous years, which highlights the frequent delays in fraud reporting. Adding to the complexity, the recovery rate of money lost to fraud remains below 1% at a mere USD 154 million. As per a Local Circles survey conducted in October 2021, 42% of Indians reported that they experienced financial fraud and 74% of them could not recover their losses within the past three years.

Banks and other financial service providers continue to make substantial investments in technology to detect and prevent fraudulent transactions. One effective approach is artificial intelligence (AI) techniques and machine learning (ML) tools to combat both existing and future fraud.

As per research by Deloitte, 73% of respondents mentioned that their banks monitor transactions continuously to enhance security. Additionally, 16% of respondents reported that their banks use AI and ML tools specifically to prevent fraud.

However, financial service providers are not the only ones to rely on AI and ML to combat fraud. Fraudsters themselves have been exploiting these technologies. Armed with generative AI tools, they craft a complex web of counterfeit content that uses text, images, and videos to trap unsuspecting victims. This highlights the need for unyielding vigilance and a continuous evolution of strategies to outpace the ever-evolving instances of fraud.

MSC conducted qualitative research in Delhi to unpack the issue of rising financial fraud and understand the perspective and experience of DFS users and financial service providers. The research sought to inform comprehensive policy recommendations on fraud that affects DFS in India. This policy brief draws on respondents' experiences, including those who safeguarded themselves against fraud or fell victim to fraud and lost money. The brief also captures the experiences of DFS fraud victims as they made complaints, sought post-fraud recovery of their money, and used DFS after experiencing fraud.

Key insights

The research found **little correlation between education or income levels and DFS fraud**. However, a correlation did appear between fraud awareness levels and incidents or attempted incidents of fraud. Among DFS users, those with a high level of awareness about DFS and fraud trends were less likely to fall victim to fraudulent attempts, while victims of fraud were observed to have lower DFS and fraud-related awareness.

- **The most prevalent types of fraud are those that involve respondents who shared their one-time password (OTP) or those related to** Unified Payments Interface (UPI). Based on our research findings, 32% of individuals were deceived into sharing an OTP with fraudsters, 24% of respondents experienced UPI-related fraud, and 20% fell victim to link phishing.
- The majority of fraud victims expressed **lower confidence in DFS** after they experienced fraud. DFS users who have encountered fraudulent attempts or are aware of it reported they adopted a more cautious approach during online transactions through DFS platforms after the incident.
- Respondents who use DFS for their business consider it an important tool for their work. They continue to use DFS even after they encounter fraud. However, these individuals often lose trust in their current financial service providers (FSPs) due to fraud and switch to a new FSP for their DFS needs.
- The predominant source of information on trends in DFS fraud, grievance resolution mechanisms (GRMs), and cautionary information is through informal communication channels. **WhatsApp stands out as the platform the DFS user community uses the most to share and exchange information**. Other sources of information include the Internet, social media platforms, and news articles.
- The recovery rate of money lost to fraud is remarkably low, which can be attributed primarily to the limited awareness of the available GRMs and victims' reluctance to file complaints for fear of humiliation within their community. Institutional support for the registered complaints is slow and inefficient due to inefficient coordination between banks and the cyber-crime reporting cell. **Officials noted that the main reasons for low recovery rates are delays in making the complaint, inefficient complaint resolution systems, and the lack of dedicated resources available to address the growing number of fraud cases**.
- Most female respondents report that they hesitate to approach authorities and report fraud without a male family member present. They perceive the reporting process as a hassle, as repeated questioning and multiple visits take a toll on them. Additionally, most female and elderly respondents who have experienced fraud subsequently depend on their children or male family members to conduct online financial transactions. Insights from officials further confirm that **fraudsters view women and elderly individuals as easier targets**.

Detailed findings

The risk of DFS fraud largely depends on the user's level of awareness.

The study findings indicate that high awareness levels of consumer risks in DFS, past experience, and strong digital skills are key for users to safeguard against financial fraud in DFS. Users with high awareness of emerging fraud are more equipped to recognize and avoid potential threats. Those who have encountered fraud earlier or know fraud victims exhibited increased caution when they used DFS. Additionally, users with strong digital skills could navigate platforms securely, identify risks, and implement effective security practices. This means that knowledge of DFS and related frauds plays a more important role in deterring frauds, than general education levels. As per bank officials, individuals with high education and income levels who use DFS are also at risk of falling victim to fraud.

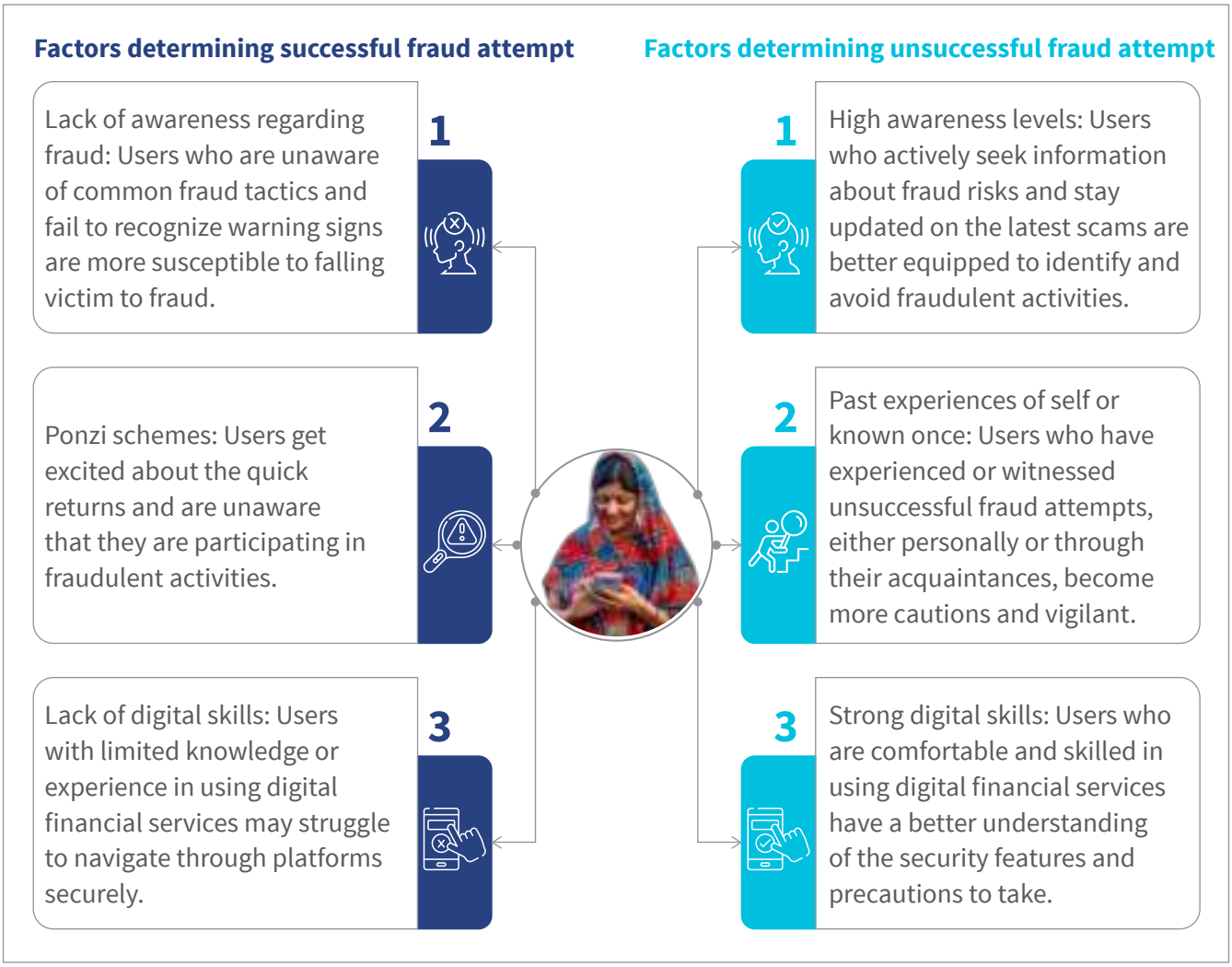


Figure 1: Factors that determine successful or unsuccessful fraud attempts.

Case study 1:

Awareness built through mass media campaigns safeguarded Mahendra from financial fraud

Mahendra is a corner shop owner who studied until the sixth standard. He is a DFS user who safeguarded himself against a fraud attempt. He received a call that he had won a lottery, after which the caller sent him INR 1 on his UPI as a show of trust. He asked Mahendra to reciprocate and upon doing so, he received an OTP for which the caller wanted him to relay. However, Mahendra recalled instructions not to share OTPs with a third party and identified the caller as a scammer. While Mahendra has only completed primary education, he remains updated about fraud trends through social media and through exchanges with his friends.

Fraudsters exploit patriotic and emotional sentiments to deceive DFS users.

The research mapped the different types of fraud to understand common trends. As seen in Figure 3, OTP-related fraud is the most common, followed by UPI-related fraud, and link phishing. Digital fraud seems to be the most common because of the changing e-commerce landscape, which has led more and more digitally naïve users to turn to online platforms and digital transactions.

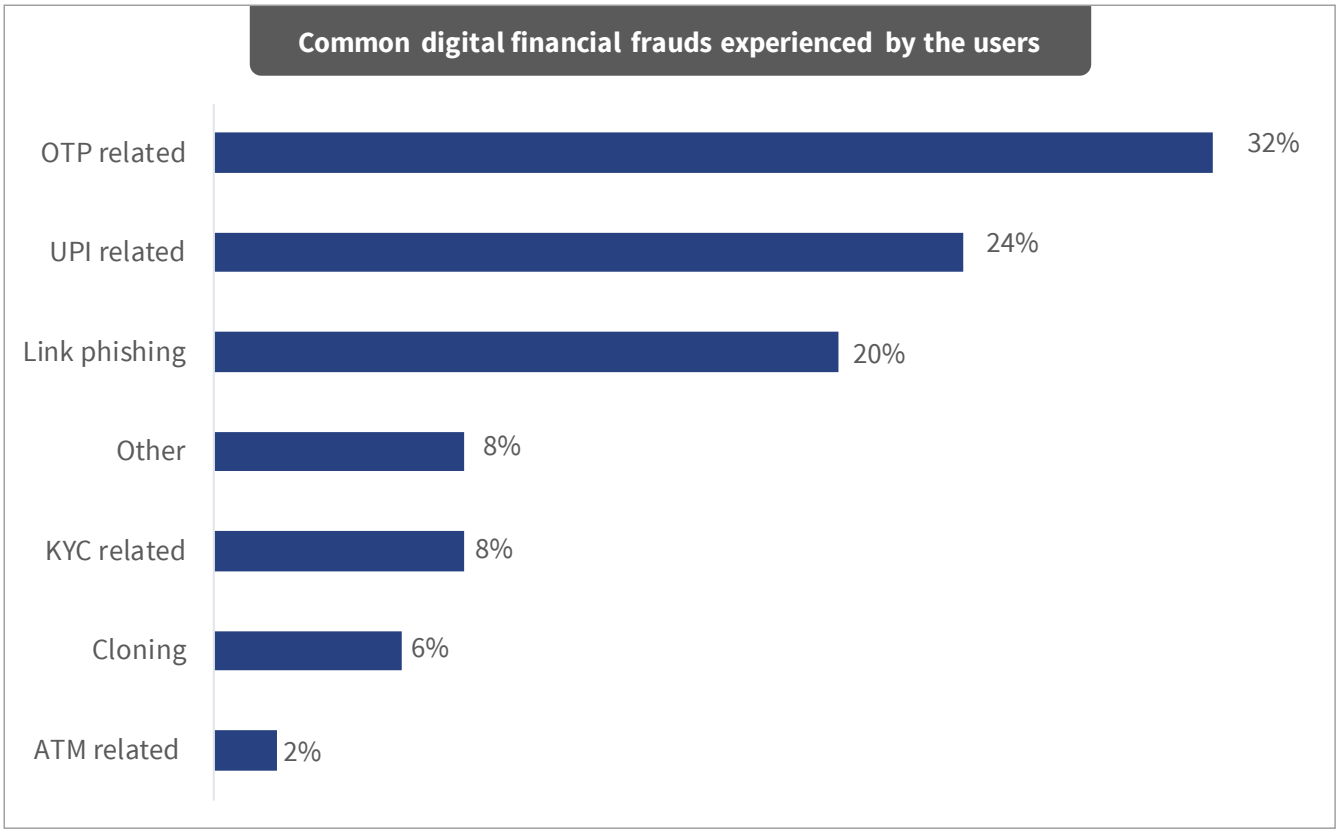


Figure 2: Common types of fraud

Fraudsters convince the majority of victims to reveal their personal details. They also exploit the patriotic sentiments of DFS users by posing as retired army officers who need financial aid or are trying to make a sale or purchase on a thrift e-commerce platform, such as OLX, where people can buy secondhand items personally from the seller. They also promise to return or deliver a service in exchange for money transfers. Consequently, many victims fall for this fraud and lose their money. Many such individuals realize they have become victims of fraud only after they transfer the money. Another common trend respondents reported is when fraudsters pretend to be distressed relatives or friends who need urgent financial assistance.

Breach of data privacy at various levels contributes significantly to fraud.

Fraudsters use personal financial information and past transactions to gain victims' trust and access their OTPs and financial data. They often trick people with fake job offers or false account closure notifications, which lure victims to click harmful links or share OTPs and incur financial losses. People can learn to detect such scams and protect themselves when informed about others' experiences.

Case study 2:
Playing with patriotic sentiments for personal gain

Phuntso is a local business owner in Majnu ka Tila, North Delhi. He believes that DFS fraud is common in his community. He knows several people who have been defrauded. One such case was an attempt of fraud when the fraudster posed as a retired army official and contacted Phuntso's friend to purchase chicken from his shop. He promised to pay after the chicken was delivered, but because Phuntso knows of fraudulent trends, he warned his friend to ignore the order. The fraudster attempted to manipulate his friend's patriotic sentiments by claiming to be a virtuous civil servant, yet thanks to Phuntso's intervention, his friend was not defrauded.

Case study 3:
The promise of a new job

Shefali, a homemaker, and her 17-year-old daughter, Tanya, visited a cyber cell in South Delhi to lodge a complaint about a recent instance of fraud. Shefali reported that she had recently lost a job as a gig worker in a private company and was applying for new employment opportunities when she received a call from someone claiming to be a representative of Natraj pencils offering her a job. She believed that she was receiving a call back from a previous employment application. The fraudster convinced her to pay an advance of INR 15,000 (USD 182) to move the application forward, with the promise of an INR 30,000 (USD 364) salary per month. However, with Tanya's help, Shefali realized that the representative was trying to scam her. Yet by then, she had made a series of UPI payments and lost money. Shefali attributed the fraud to her lack of awareness and digital literacy, and because she desperately needed a job.

Fraud victims exhibit decreased confidence in DFS channels after they experience fraud.

The majority of respondents reported decreased levels of confidence in DFS after they experienced fraud. Notably, fraud victims switch platforms after they experience fraud. They may move from Paytm to Google Pay, for instance. All respondents report that after fraudulent attempts, they are more cautious when they use DFS platforms or click on unknown strange links.

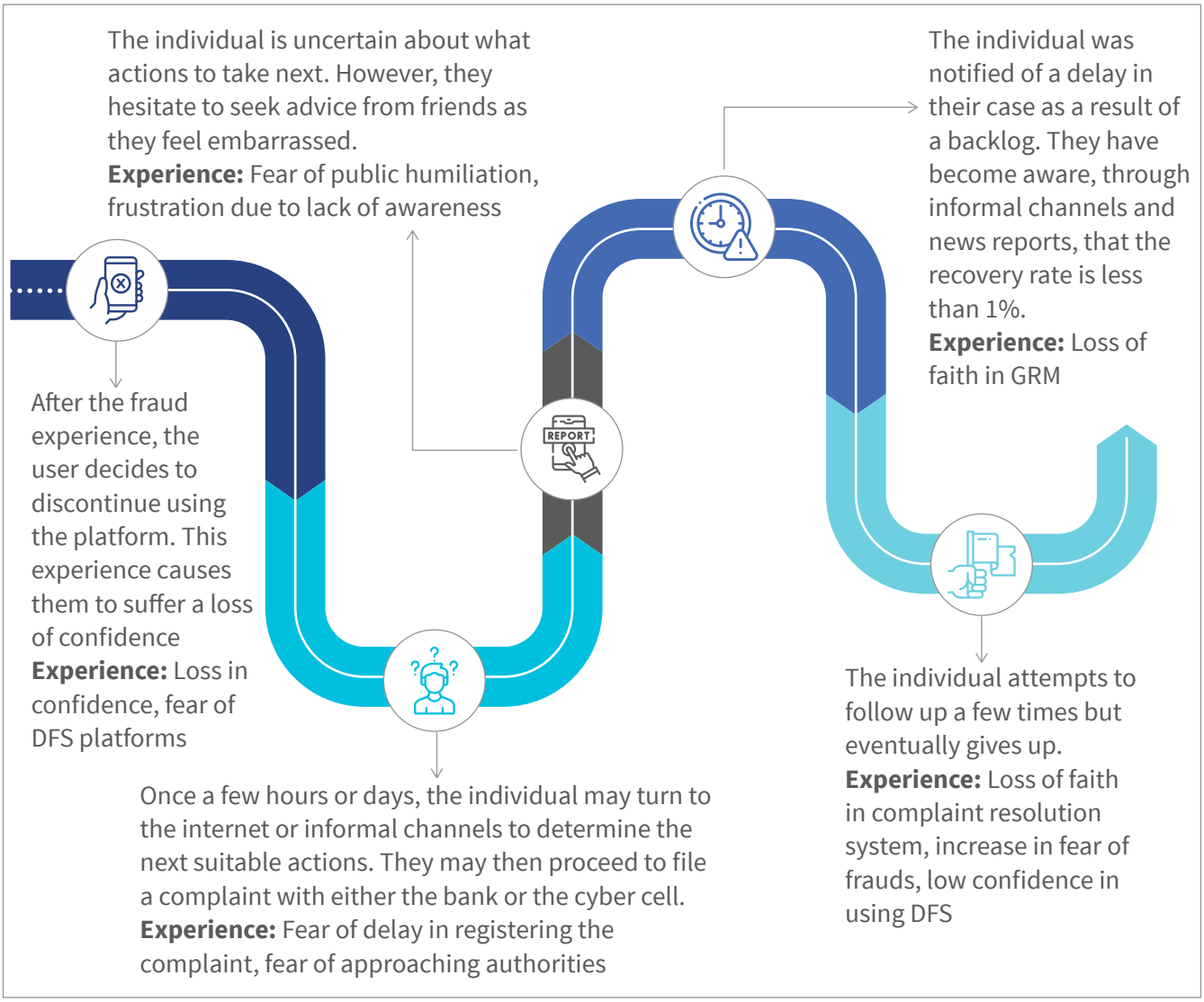


Figure 3: Experience of DFS fraud victims post fraud

Case study 4:
Switch of DFS platform after an experience of fraud

Priyanka is a frequent DFS user and is confident in her use of online platforms for financial transactions. However, she does not use Paytm anymore after her balance was mysteriously deducted on the app. She searched the Internet for ways to resolve her issue, and registered her complaint with customer service and the fraud was identified as a case of link phishing. As Priyanka unknowingly clicked on a link, she was not able to recover her money. She reported that although she continues to use DFS platforms for financial transactions, she has not used Paytm after the fraud incident, and now prefers alternatives, such as Google Pay. She is also more cautious about clicking unknown links and sharing OTPs.

DFS fraud victims hesitate to share experiences within the community.

Some individuals who fell victim to fraud hesitate to share their experiences (Figure 4), particularly women who hesitate to file complaints without the presence of a male family member. Priyanka (case study 4) recounted how she hesitated to approach the authorities because she knew her case would only be registered after several visits and repeated questioning. She believes the process is too intimidating, time-consuming, and lacks tangible outcomes. Phuntso (case study 2) mentioned that his close-knit community includes several elderly members, and they hesitated to disclose details about fraud to external individuals. He also mentioned that people do not want to use complaint resolution channels due to a lack of trust.

MSC's research team asked respondents about their social media platform use to gauge their access to information on DFS platforms, fraud trends, and GRM processes. All the respondents reported they used WhatsApp, followed by 68% who prefer Instagram for information, while 58% use Facebook. This response emphasizes the role social media plays to spread awareness, especially for younger generations.

Case study 5:
Social media helps spread targeted information

Shambhavi, a college student, helped her mother avoid being defrauded when her mother received a call from a fraudster who claimed that her bank account was closing and her OTP was needed to resolve the issue. Shambhavi warned her mother against sharing the OTP and immediately contacted the cyber cell. She attributed this to the workshops in her university on fraud prevention, as well as a video on fraud she saw on Instagram.

Fraud victims hesitate to approach authorities due to delays in the complaint resolution process and low recovery rates.

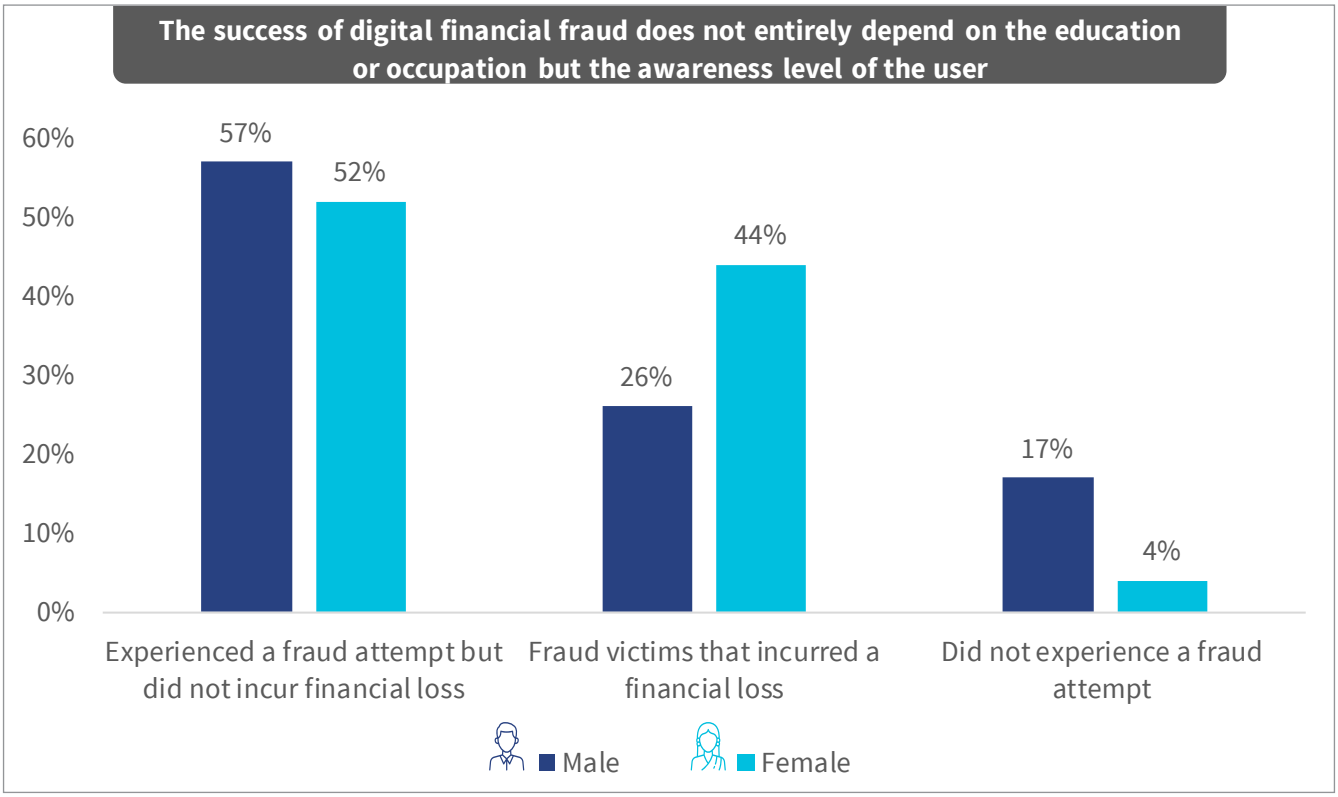
The majority of respondents reported they could not recover the money they lost, even though they had lodged formal complaints with the authorities. Cyber cell officials attribute delays in the resolution process to a spike in DFS fraud and cybercrimes, as well as the time taken to report the fraud after it occurs, which typically results from a lack of awareness of the GRM process. The source of fraud is easier to track if it is reported within a specific timeframe, usually 24-48 hours. Bank officials also mention that in most cases, the perpetrators withdraw the money by the time fraud victims report the fraudulent activity.

In Chandigarh, bank officials explain that a significant number of individuals lack awareness of preventive measures against fraud. Consequently, when they face a fraud attempt, many become apprehensive and opt to close their bank accounts.

Fraudsters find it easier to target specific groups, such as the elderly and women.

Cybercrime officials emphasize that while DFS fraud affects users across segments, the elderly are most impacted due to their lack of digital literacy and access to information about fraud trends. “This makes them an easy target for complex fraud, as they are scared easily and end up sharing OTPs with fraudsters,” said a bank branch manager.

Women are the other easy target for fraudsters, especially since many female respondents claimed they prefer to rely on their husbands or technologically-aware children to conduct online transactions and glean information. Ritu, a small business owner, said that although she handles customers and runs a business, she prefers her husband handle online transactions with suppliers and large-scale orders.



Areas with recent internet connectivity experience increasing incidents of fraud.

A noticeable trend and familiar patterns of fraud have emerged in areas where internet connectivity has been introduced relatively recently, such as the Andaman and Nicobar Islands, where the Chennai-Andaman & Nicobar Islands (CANI) cable was inaugurated in 2020. Cybercrime officials have noted a resurgence of older fraud tactics, such as phone mirroring and deceptive link downloads, which take advantage of the newly established digital connections in the region.

Since the local population has encountered these fraud trends for the first time, they are more vulnerable to the traditional tricks employed by fraudsters. Consequently, the Andaman and Nicobar Islands have seen a significant rise in digital fraud cases. Cybercrime officials have been working to trace the perpetrators, often located in states, such as Bihar and Haryana. Additionally, the officials highlight that due to the recent integration of Internet services, residents are less accustomed to electronic money transfers and are more susceptible to intimidation by fraudsters.

Recommendations

Our research highlighted that most people could safeguard themselves against fraud better if they were aware of the evolving trends of fraud. MSC suggests implementing a three-tiered approach to enhance user awareness, which is inversely related to instances of fraud. This approach would encompass large-scale, community, and individual-focused initiatives to enhance knowledge, attitude, skills, and action to protect against financial fraud:

Framework	Large-scale	Community	Individual
Knowledge	Mass communication campaigns by DFS providers, regulators, and the government	Community-based awareness campaigns by cybersecurity ambassadors	Targeted text or IVRS to deliver personalized information initiated by DFS providers through social media platforms
Attitude	Train ambassadors who can run regional language campaigns to share emerging trends in fraud. An emphasis on storytelling may motivate victims to share their experiences and change their overall attitude toward fraud	Partnerships with schools and universities to shift the mindset of both students and adults about using DFS platforms safely	Collaboration between DFS providers and WhatsApp to create an interactive voice-based chatbot that can offer information on various fraud types and best practices. It would also have a cybercrime helpline for users to lodge complaints, which would help users who hesitate to approach authorities
Skills	Bank agents, whom customers often approach to resolve issues, can be skilled and incentivized to promote responsible financial practices	Promote training and engagement of community ambassadors, such as village panchayat leaders and self-help group leaders, among others, to enhance digital skills and promote responsible financial practices	Collaboration with social media platforms, such as WhatsApp, to increase user skills in responsible financial practices
Action	Create a fund for risk mitigation and prevention where all players in the DFS industry contribute. This will help coordinate actions to tackle the increasing risks related to consumer protection	Offer rewards or acknowledgments to community leaders and cybercrime officials for their contributions to reduce financial fraud. Recognizing their efforts and sharing their stories will encourage ongoing dedication to combat the increasing issue of financial fraud	Initiate confirmation pop-ups before DFS transactions to actively prevent fraud

Figure 4: Summary of recommendations

1. Mass communication campaigns

Large-scale targeted campaigns are essential to maximize outreach. These campaigns can be run on social media platforms, DFS applications, and through television and radio broadcasts. These efforts intend to raise awareness of preventive measures against fraud and ensure a broad audience is well-informed and vigilant. The Reserve Bank of India launched a multimedia campaign, "RBI Kehta hai," in 14 languages to educate the public about safe banking and financial practices.

The campaign achieved tremendous success and gained widespread popularity. This marked the first instance of a comprehensive 360-degree campaign launched by the central bank that used various mass media channels, such as television, radio, newspapers, billboards, web banners, GIFs, social media, and SMS.

Mass media campaigns have proved crucial to enhance financial literacy for pension planning in Kenya. They were similarly effective in raising awareness of COVID-19. These types of interventions have clear potential to help create widespread awareness of safe and responsible financial practices in India.

2. Employing community ambassadors to prevent fraud

At present, cyber cell officials hold workshops and seminars for youth to increase awareness of fraud trends and suggest preventive measures. For widespread impact, we recommend training cyber-security community ambassadors who can lead similar campaigns in regional languages to raise awareness of current and emerging fraud trends and provide advisory services in times of distress. They could also facilitate and enable storytelling so that victims feel comfortable to share their experiences.

The ambassadors can work with organizations, organize cyber-security seminars, and disseminate information to communities to enable them to implement protective measures against digital financial fraud. These organizations could include colleges, schools, vendor associations, and self-help groups (SHGs).

1. Use of regional language

The ambassadors communicate in regional language to make people aware of emerging frauds.

2. Use of storytelling

The ambassadors facilitate a storytelling platform where victims can share their experiences of financial fraud and preventive measures.

3. Stakeholder management

Ambassadors work together with different organizations, including colleges, schools, vendor associations, and self-help groups (SHGs).

Figure 5: Cybersecurity community ambassador model

Additionally, bank agents can play a major role to raise awareness of responsible financial practices. As customers often approach agents to seek information and resolve issues, these agents can be trained and incentivized to actively promote responsible financial behaviors and provide information that safeguards customers from potential financial risks. MSC's collaboration with CGAP underscores how agents can effectively protect customers from such risks and emphasizes their crucial role.

2. Targeted awareness initiatives through WhatsApp integrated into DFS platforms

100% of respondents report they feel comfortable using WhatsApp, and research suggests that communication channels, such as WhatsApp, are the most common source to obtain information on fraud trends and the complaint resolution process. MSC suggests a collaboration between WhatsApp and DFS providers to develop an interactive feature to improve users' awareness levels.

The prototype for this feature would comprise an interactive voice-based chatbot integrated into the system. This chatbot would provide users with convenient access to information on current fraud trends and ways to seek complaint resolution. The chatbot's built-in capabilities would encompass details on various fraud types, best practices to prevent fraud, and an interactive simulator to allow users to practice their responses in simulated fraudulent situations.

The chatbot would also offer access to a cybercrime helpline mechanism to streamline the process to register complaints. This would especially benefit users who hesitate to contact authorities immediately and reduce any unnecessary hassle for them.

1. Awareness

The chatbot alerts users through real-time updates and proactive alerts about the latest scams, phishing attempts, and identity theft techniques

2. Practice

This features users' test skills and helps them stay sharp with the updated with stimulated scam scenarios, phishing attempts, and identity theft challenges.

3. GRM process

The chatbot simplifies the complex journey of reporting and resolving fraudulent activities.

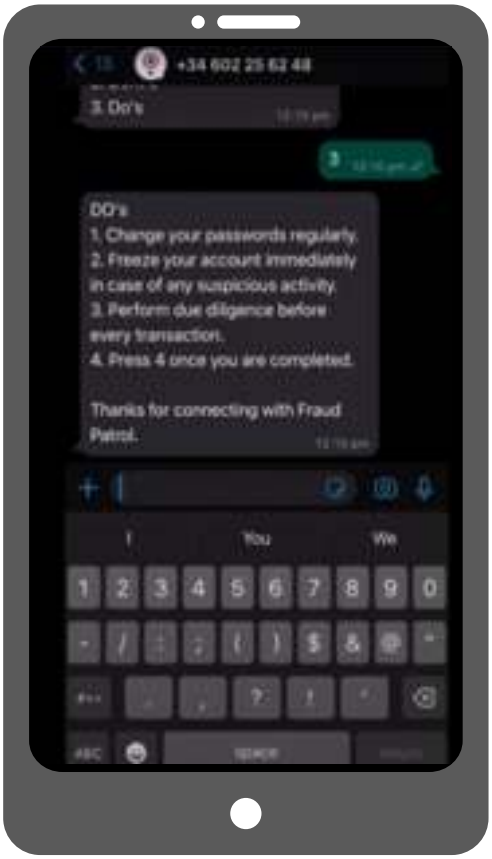
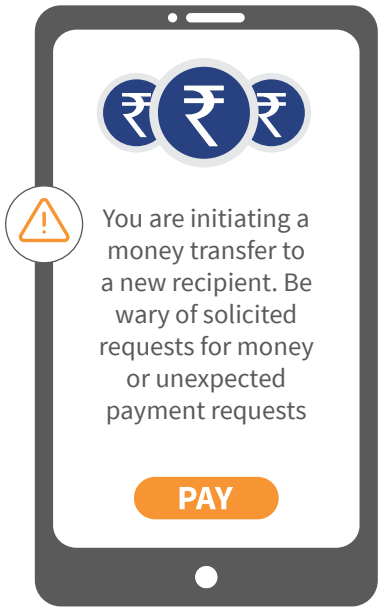


Figure 6: Example of API/chatbot

Further, we can integrate SMS pop-ups or IVR messages to advise users not to transfer funds to unfamiliar numbers. This proactive approach ensures consistent reminders for users to protect their information during digital transactions. A similar method known as Hakikisha is already in use for transactions using M-PESA in Kenya. This allows customers to confirm the name of the person they want to send money to before they finalize a transaction.



Communication - At individual level

Conclusion

As digital transformation accelerates, we will see a rise in risks, fraud, cyberattacks, digital privacy breaches, and disruptions to the interconnected digital infrastructure, which could lead to financial losses at the household level. These attacks will disproportionately affect low-income customers who lack access to suitable information channels and knowledge of the evolving and increasing DFS consumer risks. This will lead to increased disputes and grievances alongside eroded trust in DFS.

Most first-time DFS users, especially those who lack digital awareness or digital skills, struggle to understand and navigate the complaint resolution process. DFS providers should adopt innovative approaches outlined above through a combination of grassroots outreach and technology to reach the mass market and thus reduce DFS consumer risks and help build a responsible financial ecosystem.

Research background

MSC sought to understand the experiences of DFS users subject to digital financial fraud and conducted a qualitative research study[1] with 50 respondents spread across different parts of New Delhi. The respondents interviewed came from a range of socioeconomic backgrounds and occupations.

We also held consultations with 10 institutional stakeholders (cyber cell officials and bank officials) in Delhi, Chandigarh, and the Andaman and Nicobar Islands. Through these consultations, we sought to understand their perspectives on the current and emerging fraud trends, as well as reasons behind the low recovery rates. These interviews sought to understand financial service providers' perspectives to inform more comprehensive policy recommendations.

Number of respondents: 50

Female = 27 Male = 23

Salaried employee	Business/Corner shop owners	No Income	Wage labor
27	14	8	1

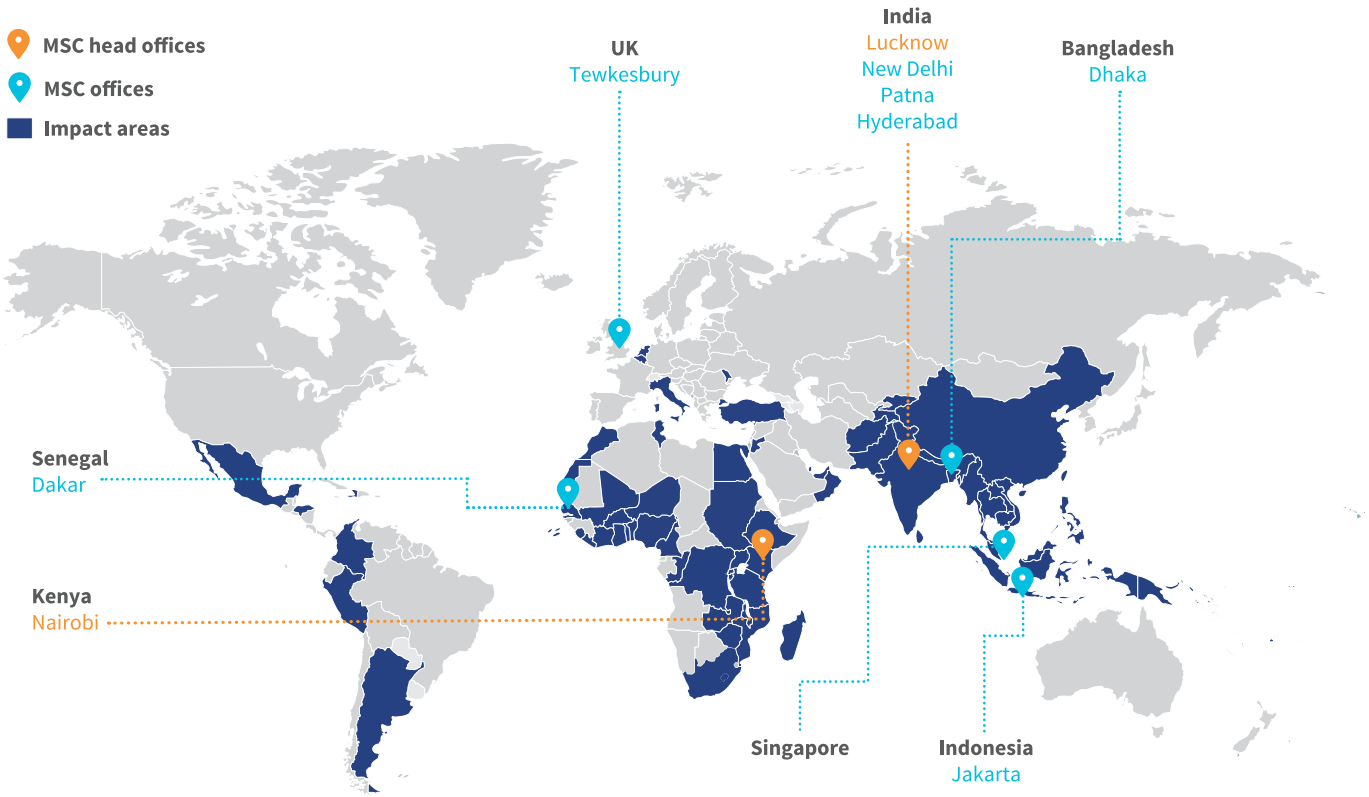
Research objectives

The objectives of the study were to:

- Understand the nature of fraud experienced by DFS users;
- Map the reasons behind DFS frauds; and
- Assess the efficiency of grievance redressal mechanisms (GRM) and institutional support for the recovery of monies lost.

[1] Notably, the study is qualitative in nature. The percentages presented are indicative. The sample size for this study was relatively small (N=50), which limits the generalizability of the conclusions. The results should be used with caution.

MSC
MicroSave Consulting



Asia head office

28/35, Ground Floor, Princeton Business Park, 16 Ashok Marg,
Lucknow, Uttar Pradesh 226001, India
Tel : +91-522-228-8783 | Fax : +91-522-406-3773
Email : manoj@microsave.net

Africa head office

Landmark Plaza, 5th Floor, Argwings Kodhek Road
P.O. Box 76436, Yaya 00508, Nairobi, Kenya
Tel : Tel: +254-20-272-4801/272-4806
Email : anup@microsave.net

www.microsave.net