The Dialogue®
INFORM ENGAGE IDEATE

dlai

CUSTOMER PROTECTION IN THE DIGITAL LENDING ECOSYSTEM IN INDIA

A White Paper Developed with the Joint Expertise of The Dialogue and The Digital Lenders Association of India (DLAI)

WHITE PAPER

Customer Protection in the Digital Lending Ecosystem in India

Copyedited by : *Akriti Jayant*

Thematic Design by : *Shivam Kulshrestha*

The Dialogue® is a public policy think tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue ᴿ has been ranked as the world's Top 10 think tanks to watch out for, by the Think Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

The Digital Lenders Association of India (DLAI), established in October 2016, is a national industry association for fintech entities including digital lending companies. As a not-for-profit Section 8 company, DLAI promotes responsible lending, consumer protection, and innovation in the fintech space. Representing almost 100 fintech entities, it maintains high standards of corporate governance with 33% independent directors on its board, chaired by an Independent Director.

The primary objective of DLAI is to establish ethical and transparent fintech service delivery practices within the financial inclusion space. By developing and promoting an Industry Code of Conduct (COC), DLAI ensures that its members adhere to the highest standards of customer service, data privacy, and fair lending practices. This commitment to responsible fintech is instrumental in building trust among consumers and regulators alike.

As the fintech ecosystem continues to evolve, DLAI remains at the forefront of shaping the industry's development and represents customer centric and industry views. DLAI's commitment to fostering responsible lending practices, advocating for regulatory clarity, and promoting collaboration positions it as a key player in driving the positive transformation of India's fintech landscape. In essence, DLAI serves as a cornerstone for the industry, championing ethical conduct, innovation, and inclusivity in the rapidly expanding domain of fintech in India.

For more information
https://thedialogue.co | https://www.dlai.in/

Suggested Citation
Customer Protection in the Digital Lending Ecosystem in India (2024, August). The Dialogue®

Catalogue No
TD/DE/WP/0824/02

Publication Date
August 27, 2024

Contents

1 INTRODUCTION

The Indian financial landscape has recently witnessed a critical development: the advent of digital lending companies. This evolution in India is driven by the rise of fintech companies that provide convenience and accessibility to consumers.[1] Digital lending is a remote and automated lending process that uses seamless technologies for customer acquisition, credit assessment, loan approval, disbursement, recovery, and associated customer service.[2] Companies providing these services include fintech companies such as Loan Service Providers (LSPs), Non-Banking Financial Corporations (NBFCs), and digital arms of traditional banks, which provide user-friendly websites and mobile apps for loan applications.[3]

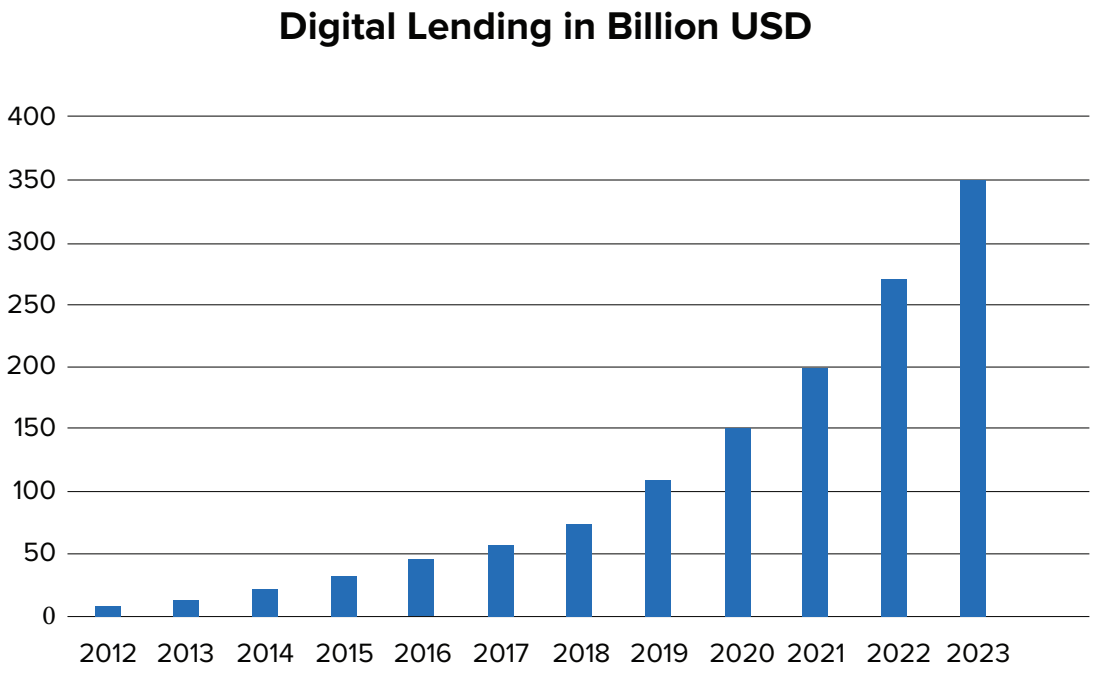


Figure 1: Value of digital lending market in India from 2012 to 2020, with estimates until 2023 (in billion U.S. dollars)[4]

[1] Lancelot Joseph, 'Rise and Rise of Fintech' (Business India, 5 April 2023) <https://businessindia.co/magazine/rise-and-rise-of-fintech> accessed 30 July 2024.
[2] 'Guidelines on Digital Lending' (RBI, 2 September 2022) <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/GUIDELINESDIGITALLENDINGD5C35A71D8124A0E92AEB940A7D25BB3.PDF> accessed 30 July 2024.
[3] 'Digital Lending in Depth' (Razorpay, 11 October 2023) <https://razorpay.com/learn/business-banking/digital-lending/> accessed 30 July 2024.
[4] 'Value of digital lending market in India from 2012 to 2020, with estimates until 2023', (Statistica) <https://www.statista.com/statistics/1202533/india-digital-lending-volume/ > accessed 30 July 2024.

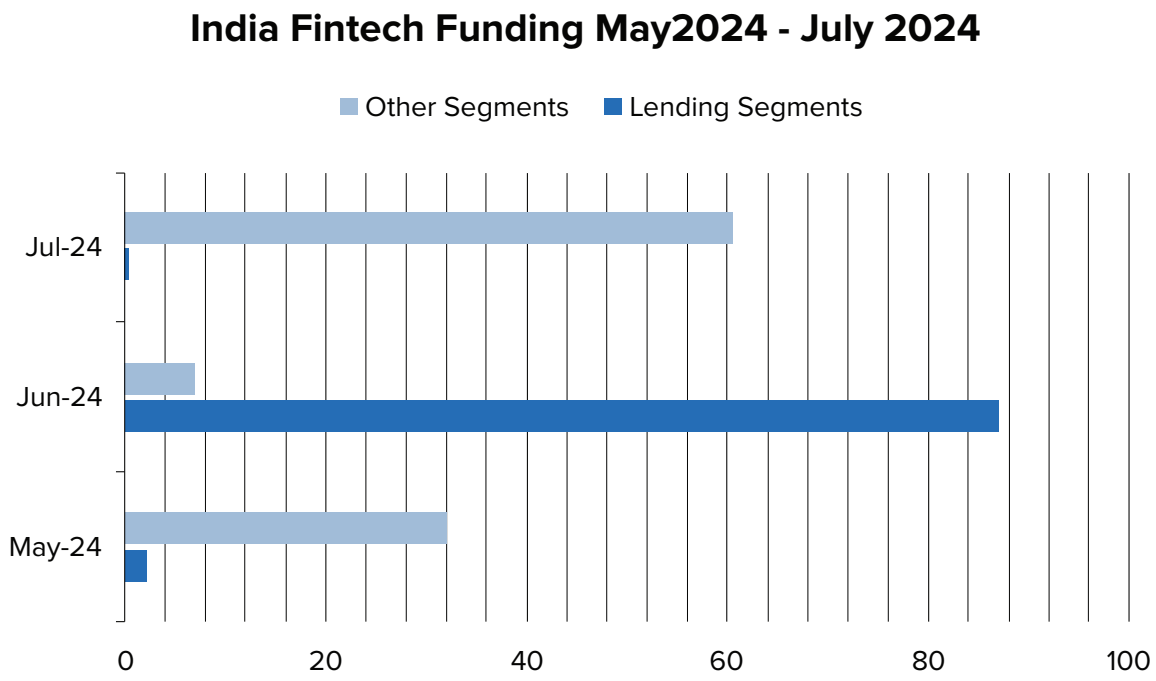


Figure 2: Investment in Fintech funding in May 2024,[5] June 2024[6] & July 2024[7]

The digital lending landscape has expanded remarkably in recent years. From 2012 to 2020, the market value in India surged from 9 billion U.S. dollars to nearly 150 billion dollars. Furthermore, as shown in Figure 2 above, in June 2024, the digital lending sector received over 80% of the fintech sector's total funding.[9] Along with this rapid growth, the sector has also faced significant challenges. The rise of unauthorised lending apps, social engineering scams, and cybercrime has increased risks for customers, undermining their protection and eroding trust in digital lending.[10]

Cybersecurity concerns in the digital lending sector have caused financial losses amounting to ₹1.25 lakh crore in recent years, underscoring the scale and severity of the issue.[11] Furthermore, after studying the digital lending apps ecosystem in January and February 2021, the Reserve Bank of India (RBI) revealed that out of 1,100 loan apps available on 81 app marketplaces, 600 were operating illegally.[12] Additionally, the impact of these cyber crimes is evident in the statistics: in 2022, digital lending app-related frauds totaled 26,844 cases, and there were 9,926 cases in 2023.[13]

This research initiative aims to explore solutions to mitigate these challenges and enhance customer protection within the Indian digital lending sector. The report aims to identify and address gaps that expose consumers' vulnerabilities. Further, the report will

5. 'India Fintech Funding May 2024', (The Digital Fifth, May 2024) <https://thedigitalfifth.com/indian-fintech-funding-report-2024/> accessed 20 August 2024
6. 'India Fintech Funding June 2024', (The Digital Fifth, June 2024) <https://thedigitalfifth.com/indian-fintech-funding-report-june-2024/ > accessed 20 August 2024
7. 'India Fintech Funding July 2024', (The Digital Fifth, July 2024) <https://thedigitalfifth.com/indian-fintech-funding-report-july-2024/ > accessed 20 August 2024
8. 'Value of digital lending market in India from 2012 to 2020, with estimates until 2023', (Statistica) <https://www.statista.com/statistics/1202533/india-digital-lending-volume/ > accessed 30 July 2024.
9. 'India Fintech Funding June 2024', (The Digital Fifth, June 2024) <https://thedigitalfifth.com/indian-fintech-funding-report-june-2024/ > accessed 20 August 2024
10. 'Indian consumers still vulnerable to being tricked by illegal loan apps' (Economic Times, 16 April 2024) <https://bfsi.economictimes.indiatimes.com/news/financial-services/indian-consumers-still-vulnerable-to-being-tricked-by-illegal-loan-apps-report/109336192#:~:text=Over%20three%2Dfourths%20of%20users,reputation%20of%20responsible%20digital%20lenders> accessed 30 July 2024.

develop practical recommendations for strengthening the digital lending sector in India.

To explore security gaps in the digital lending sector and find solutions that can mitigate them, the Digital Lenders Association of India (DLAI) and The Dialogue launched the research initiative *'Customer Protection in Digital Lending'*. The initiative, culminating in this white paper, explores problems and solutions through secondary research and stakeholder consultations. Importantly, the following consultations took place:

1. **Customer Protection in Digital Lending (Delhi):** On 21 February 2024, a stakeholder consultation was conducted, providing a platform for digital lending companies, industry players, technological solution providers, civil society, and government representatives to discuss issues in the sector.
2. **Customer Protection in Digital Lending: Way Forward (Bengaluru):** Subsequently, the second discussion was organised on 16 April 2024, where representatives from digital lending enterprises, cybersecurity experts, civil society, the government, and technological solution providers came together to discuss solutions for existing challenges.

This white paper presents insights and recommendations from these stakeholder consultations, as well as secondary literature. Chapter 1 of the paper provides context on the subject. Chapter 2 examines the *status quo* of customer safety in the Indian digital lending space. Chapter 3 explores security concerns and available solutions. Chapter 4 investigates potential reasons for the low adoption of technological solutions by digital lending companies. Finally, Chapter 5 proposes a way forward and provides recommendation for each stakeholder to address these issues in the digital lending ecosystem.

[11] Sunainaa Chadha, 'Explained: Types of payment frauds and what to do if you lose money' (Business Standard, 27 June 2024) <https://www.business-standard.com/finance/personal-finance/-explained-types-of-payment-frauds-and-what-to-do-if-you-lose-money-124062700361_1.html> accessed 30 July 2024.

[12] ''Debtly Sins: Illegal loan apps are a menace. Killing their business requires quick prosecution, more competition' (The Times of India, 28 December 2023) <https://timesofindia.indiatimes.com/blogs/toi-editorials/debtly-sins-illegal-loan-apps-are-a-menace-killing-their-business-requires-quick-prosecution-more-competition/#:~:text=RBI%20studied%20DLAs%20over%20two,many%20as%20600%20were%20illegal> accessed 30 July 2024.

[13] ''The fintech industry and cyber security: Rising incidences of white collar crimes' (Financial Express, 7 August 2023) <https://www.financialexpress.com/business/banking-finance-the-fintech-industry-and-cyber-security-rising-incidences-of-white-collar-crimes-3202495/> accessed 30 July 2024.

2 Overview of Security Concerns in Digital Lending

The rapid expansion of digital lending in India has been impacted by a proliferation of security concerns that threaten customers and institutions. This chapter delves into the three primary concerns prevalent in the sector: unauthorised lending apps, social engineering scams, and cybersecurity issues.

2.1. Unauthorised Lending Apps

Unauthorised lending apps have emerged as a significant threat in the digital lending landscape.[14] Fake lenders impersonate legitimate institutions, often offering quick credit with minimal documentation, sometimes bypassing proper Know Your Customer (KYC) and income assessments. Their operations involve unlawfully collecting personal and financial data, charging hidden fees and interest, and imposing predatory loan terms.[15] This unauthorised data harvesting frequently leads to identity theft, unauthorised transactions, and severe privacy violations, exacerbating the financial distress of victims.[16]

The scale of the problem is evident from the numerous complaints lodged with regulatory bodies. In fiscal year 2023, the Finance Ministry received a staggering 1,062 complaints against such lending apps, highlighting the widespread nature of the issue.[17] Additionally, the RBI Report from 2021 revealed the state-wise distribution

State-wise Number of Complaints regarding unauthorised digital lending apps from jan 2020 - March 2021

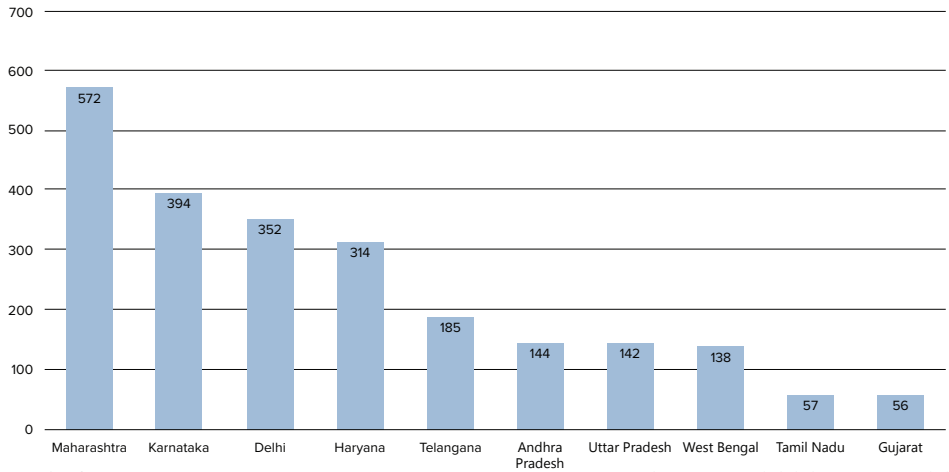


Figure 3: Complaints regarding illegal digital lending apps from Jan 2020 - March 2021[18]

[14] Abeer Ray, ' Research well before borrowing from digital lending apps, says Madhusudan Ekambaram of KreditBee' (Livemint, 6 February 2024) <https://www.livemint.com/money/personal-finance/research-well-before-borrowing-from-digital-lending-apps-says-madhusudan-ekambaram-of-kreditbee-loans-interest-rates-11707139768473.html> accessed 30 July 2024.

[15] 'Sachin Kumar, 'Stay Vigilant against illegal loan apps that lure borrower' (TNIE, 18 September, 2023) <https://www.newindianexpress.com/business/2023/Sep/18/stay-vigilant-against-illegal-loan-apps-that-lure-borrower-2615999.html> accessed 30 July 2024.

[16] Kriti Jha , '7 reasons why it is essential to stay cautious of digital lending apps' (Livemint, 3 August 2024) <https://www.livemint.com/money/personal-finance/7-reasons-why-it-is-essential-to-stay-cautious-of-digital-lending-apps-151690699757660.html> accessed 30 July 2024.

[17] Fake loan apps: What should investors do to protect themselves from these frivolous lending apps?' (Livemint, 26 January 2024) <https://www.livemint.com/money/personal-finance/-fake-loan-apps-what-should-investors-do-to-protect-themselves-from-these-frivolous-lending-apps-11706019783523.html> accessed 30 July 2024.

[18] Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps (RBI, 18 November 2021) <https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1189> accessed 30 July 2024

of complaints received between January 2020 and March 2021, with Maharashtra, Karnataka, and Delhi reporting the highest numbers.

In response to the growing menace of fraudulent apps, various stakeholders have taken significant measures to curb the spread.[19] For example, Google has actively monitored its Play Store, removing several unauthorised lending apps. Between April 2021 and July 2022, the Play Store removed or suspended 2,500 apps, while an additional 2,200 apps were taken down between September 2022 and August 2023.[20]

DLAI also compiled a list of its members' digital lending apps, shared it with regulatory and law enforcement agencies, and promoted it among customers.[21] Additionally, to strengthen the initiatives against the menace caused by unauthorised lending apps further, the RBI governor proposed creating a public repository of Digital Lending Apps (DLAs) based on the information provided by Regulated Entities (REs). The REs will report & update the information about their DLAs in the repository. This initiative is expected to assist customers in differentiating between authorised digital lending apps and unauthorised digital lending apps.[22]

These efforts will require further strengthening to ensure that the menace of unauthorised digital lending apps can be curtailed. Their impact on customers further highlights the insidious nature of these apps. The unlawful practices these apps adopt often lead to a vicious cycle of debt and financial instability for borrowers, exacerbating their economic vulnerabilities.[23] Additionally, the deceptive nature of these apps erodes consumer trust in digital financial services, posing a significant barrier to the broader adoption of legitimate digital lending solutions. This distrust not only hampers financial inclusion efforts but also hinders the growth and innovation potential of the fintech sector in India.[24]

2.2. Social Engineering Scams

Social engineering scams leverage psychological manipulation to deceive individuals into divulging sensitive information or making fraudulent payments, exploiting inherent human trust and vulnerability.[25] Phishing involves sending deceptive emails or messages that appear to be from legitimate digital lenders, tricking victims into revealing personal details such as passwords, credit card numbers, or social security numbers.[26] The sophistication of these scams has increased, with attackers often using tailored information to make their communications more convincing.

In the digital lending ecosystem, phishing attacks can trick borrowers into revealing their login credentials or financial information, leading to unauthorised access to their accounts. Additionally, unauthorised lending apps may create a false sense of urgency or exploit other vulnerabilities of the users to persuade them to share sensitive information.[27]

Identity theft is another pervasive threat, where cybercriminals impersonate trusted entities such as banks, government agencies, or well-known companies to access confidential data.[28] Fraudsters

19. 'RBI to set up Digital India Trust Agency to check illegal lending apps' (Business Standard, 31 March 2024) <https://www.business-standard.com/finance/news/rbi-to-set-up-digital-india-trust-agency-to-check-illegal-lending-apps-124033100152_1.html> accessed 30 July 2024.
20. 'Google removes 2,200 fraudulent loan apps from Play Store: MoS Finance' (Business Standard, 6 February 2024) <https://www.business-standard.com/india-news/google-removes-2-200-fraudulent-loan-apps-from-play-store-mos-finance-124020600968_1.html> accessed 30 July 2024.
21. 'Digital Lenders Association to release list of registered digital lenders' (Mumbai, 2024) <https://www.thehindubusinessline.com/money-and-banking/digital-lenders-association-to-release-list-of-registered-digital-lenders/article67821328.ece> accessed 20 August 2024.
22. Reserve Bank of India, 'Governor's Statement: August 8, 2024' <https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=58448> accessed 20 August 2024.
23. 'The dark world of illegal loan apps in India' (Aljazeera, 25 December 2023) <https://www.aljazeera.com/economy/2023/12/25/the-dark-world-of-illegal-loan-apps-in-india> accessed 25 August 2024
24. 'Borrowing from a digital lending app? Spot the red flags first' (moneycontrol, 2 August 2023) <https://www.moneycontrol.com/news/business/personal-finance/borrowing-from-a-digital-lending-app-spot-the-red-flags-first-11082521.html> accessed 25 August 2024
25. 'Personal Loan Scams in India And How To Avoid Them' (Aditya Birla Capital, 21 April 2024) <https://finance.adityabirlacapital.com/blogs/personal-finance/personal-loan-scams-and-how-to-avoid-them> accessed 30 July 2024.
26. 'What is Phishing? Attack Techniques & Prevention Tips' (IT Governance) <https://www.itgovernance.co.uk/phishing#:~:text=Phishing%20is%20a%20type%20of,social%20media%20or%20malicious%20websites> accessed 30 July 2024.
27. 'Fake Loan Apps Permissions - What you need to know from Android's Perspective' (Protectt.ai) <https://www.protectt.ai/fake_loan_app> accessed 20 August 2024.
28. ''Safeguarding Your Finances: The Importance of Identity Theft Protection' (Federal Bank) <https://www.federalbank.co.in/the-importance-of-identity-theft-protection#:~:text=How%20Identity%20Theft%20Occurs%3F,legitimate%20institutions%20or%20trusted%20individuals> accessed 30 July 2024.

often create fake loan apps that mimic legitimate digital lending platforms, luring users with attractive loan offers and low interest rates. Once installed, these apps request excessive permissions and access to personal data, leading victims to unknowingly provide sensitive information, which is then used for identity theft. The challenges of social engineering extend beyond the digital lending sector. In 2022-2023, banking fraud totalled INR 300 million,[29] with 96% of this amount attributed to fraudsters using forged or synthetic identities.[30]

Social engineering scams can cause substantial financial and personal losses, as individuals can face direct monetary losses, damage to their credit scores, and stress and anxiety. Similarly, businesses suffer from data breaches, financial theft, and reputational harm. The complexity and diversity of social engineering attacks make them particularly challenging to combat, necessitating comprehensive security measures, public awareness campaigns, and regulatory frameworks to mitigate their impact and protect consumers and institutions in the digital lending ecosystem.

2.3. Cybersecurity Breaches

Given the sensitive nature of data processed by fintech companies, including personally identifiable information, security breaches pose significant risks, including financial loss and reputational damage. It has been noted that financial services companies are 300 times more likely to be targeted by cybersecurity attacks.[31] If a threat actor gains access to a digital lending company's database, they can ransom the company or sell the data on the dark web. Additionally, they may use this information to conduct phishing attacks, targeted scams, and identity theft. Initial access to the data can also facilitate the deployment of malware, ransomware, or spyware.

Recently, the Controller General of Defence Accounts (CGDA) raised concerns about security breaches involving certain digital lending apps in India. The CGDA highlighted that some of these apps stored sensitive data on users' mobile phones, including those of defence personnel. The apps were reported to collect customer details such as contact information and personal credentials. It was claimed that these apps targeted defence personnel with the intent to extort both financial and sensitive information.[32]

In January 2024, a leading home lending solutions provider experienced a cybersecurity breach, allowing an unauthorised third party to access sensitive personal information of approximately 16.6 million individuals in its systems.[33] Similarly, another fintech firm faced a cybersecurity incident involving unauthorised access to its systems, which resulted in a portion of its systems going offline.[34] These incidents underscore the urgent need for robust cybersecurity measures among digital lending apps and service providers, given their handling of sensitive customer data.

These breaches highlight the broader issue of inadequate security measures protecting the data handled by certain digital lending apps. Given that these apps manage sensitive personal information, exploitation of security gaps poses serious risks to individual privacy. While these platforms have gained popularity due to their convenience, the breaches underscore the urgent need for enhanced security practices.

29. 'How To Identify Fraudulent Digital Lending Apps? Types of Lending Frauds and Their Impact' (CloudBankin, 18 July 2024) <https://cloud-bankin.com/loan-management/how-to-identi-fy-fraudulent-digital-lending-apps-types-of-lending-frauds-and-their-impact/#:~:text=And%20digital%20lending%20is%20no,one%20side%20of%20the%20coin> accessed 20 August 2024.
30. 'How To Identify Fraudulent Digital Lending Apps? Types of Lending Frauds and Their Impact' (CloudBankin, 18 July 2024) <https://cloud-bankin.com/loan-management/how-to-identi-fy-fraudulent-digital-lending-apps-types-of-lending-frauds-and-their-impact/#:~:text=And%20digital%20lending%20is%20no,one%20side%20of%20the%20coin> accessed 20 August 2024.
31. Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps (RBI, 18 November 2021) <https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1189> accessed 30 July 2024.
32. 'Key Defence Body Flags Digital Lending Apps CASHe, Toop For Potential Security Risks' (INC42, 30 January 2024) <https://inc42.com/buzz/key-defence-body-flags-digital-lending-apps-cashe-toop-for-potential-security-risks/> accessed 31 July 2024.
33. 'loanDepot Provides Update on Cyber Incident', (loanDepot, 22 January 2024) <https://investors.loandepot.com/news/corporate-and-financial-news/corporate-and-financial-news-details/2024/loanDepot-Provides-Update-on-Cyber-Incident/default.aspx> accessed 31 July 2024.
34. 'EquiLend Cyber Security Incident', (Equilend, 05 March 2024) <https://equilend.com/press-releases/equilend-cyber-security-incident/> accessed 31 July 2024.

3 Reasons for Security Concerns and Possible Solutions

This chapter delves into exploring the reasons for security concerns regarding the digital lending ecosystem in India & suggests possible solutions to tackle these concerns.

3.1. Unauthorised Lending Apps

3.1.1. Reasons for Concerns

Despite efforts to remove unauthorised lending apps from app marketplaces, the problem persists. In June 2024, several users raised concerns about an app identified as a "fake loan app" that harasses, blackmails, and accesses users' data.[35] Additionally, some unauthorised lending apps bypass the app store verification processes by distributing through APK (Android Package Kit) files or URL (Uniform Resource Locators).

These apps often present themselves as legitimate apps and use social media platforms to attract customers.[36] Once downloaded, they exploit users by offering quick loans at exorbitant interest rates, frequently including hidden fees and aggressive collection practices. The problem endures due to the constant evolution of these fraudulent schemes and the challenge of monitoring and regulating the vast digital landscape where they operate.

3.1.2. Possible Solutions

App marketplaces have policies in place to enhance user security, requiring apps to comply with their guidelines. Recently, Play Store has taken action against lending apps in collaboration with the Indian government. However, some apps still manage to bypass these guidelines, ultimately putting customers in India's digital lending space at risk.[37]

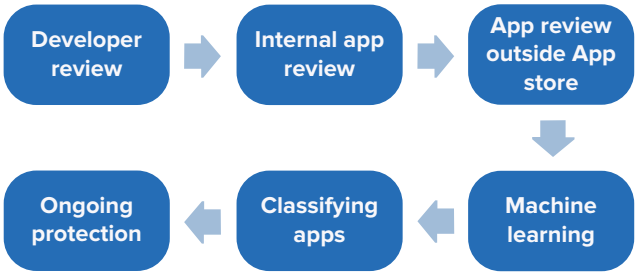


Figure 4: App review process

Some app marketplaces employ a comprehensive approach to eliminate harmful apps, including unauthorised digital lending apps, to protect users and safeguard the ecosystem. The first stage involves a "Developer review," where checks are performed on the developer's history and account details. The second stage is an internal app review, during which automated risk analysis detects potentially harmful applications. The final stage involves reviewing and analysing these apps outside the app store.[38]

Machine learning (ML) is then used to examine signals across the Android ecosystem to identify suspicious behaviour and understand the intention behind harmful applications. App marketplaces classify applications on a scale from safe to dangerous and block harmful ones. If an app manages to bypass these protections and enter the app store ecosystem, it is

35. 'Play Console Help- Community' (Google Help) <https://support.google.com/googleplay/android-developer/-thread/281802859/got-trapped-into-this-fake-loan-application-app?hl=en> accessed 31 July 2024.
36. Soumyarendra Barik, 'Fraud loan apps have a free run on social media platforms. Here's how' (The Indian Express, 27 December 2023) <https://indianexpress.com/article/business/banking-and-finance/fraud-loan-apps-have-a-free-run-on-social-media-platforms-heres-how-9033678/> accessed 31 July 2024
37. 'Ankita Chakravarti, 'Google removes 3500 loan apps in India for misleading users, violating Play Store guidelines' (India Today, 28 April 2023) <https://www.indiatoday.in/technology/news/story/google-removes-3500-loan-apps-in-india-for-misleading-users-violating-play-store-guidelines-2365919-2023-04-28> accessed 31 July 2024
38. 'Cloud-based protections' (Google Play Protect) <https://developers.google.com/android/play-protect/cloud-based-protections> accessed 20 August 2024

tracked and flagged through ongoing protection and monitoring of applications.[39]

Unauthorised digital lending apps also exploit social media to target potential victims. Social media platforms have proactively removed accounts that scammers use to deceive people into giving away money or sensitive information.[40] However, these efforts have had limited success. This indicates a need for more stringent policies for app marketplaces and social media platforms to ensure a safe and secure ecosystem for users. Additionally, continuous high-level monitoring can help identify and address emerging threats more effectively.

3.2. Social Engineering Scams

3.2.1. Reasons for Concerns

The digital lending sector is particularly vulnerable to scams due to several gaps: inadequate user awareness,[41] where many users lack awareness of common social engineering tactics, making them easy targets for phishing attacks that trick them into providing sensitive information; weak authentication mechanisms, as traditional methods like passwords and personal identification numbers (PINs) are often insufficient against sophisticated social engineering attacks. Fraudsters often use phishing or vishing (voice phishing) to obtain these credentials; and Lack of Real-Time Monitoring,[42] where existing systems often fail to provide real-time monitoring of user behaviour, which is crucial for detecting and responding to potential social engineering scams. Delays in identifying and mitigating these threats increase the risk of successful attacks.

A poorly designed user interface on apps can also further complicate matters, making it difficult for users to recognise suspicious activity or verify the authenticity of requests. Inadequate security measures, lack of user awareness, and insufficient response mechanisms are significant gaps that contribute to the prevalence of social engineering scams.

3.2.2. Possible Technological Solutions

Advanced technologies like Artificial Intelligence (AI) and Machine Learning (ML) offer promising solutions to address gaps in combating social engineering scams and cybersecurity concerns.[43] These technologies provide sophisticated capabilities for data analysis,[44] real-time monitoring,[45] and adaptive learning,[46] making them ideal for tackling challenges in the digital lending ecosystem. AI and ML can analyse user behaviour to detect anomalies and identify potential social engineering scams by continuously monitoring transaction patterns and user interactions, flagging unusual activities that deviate from typical behaviour.[47]

39. 'Cloud-based protections' (Google Play Protect) <https://developers.google.com/android/play-protect/cloud-based-protections> accessed 20 August 2024
40. 'Avoid scams on Instagram' (Instagram Help Center) <https://help.instagram.com/514187739359208> accessed 31 July 2024.
41. 'Cybersecurity 2.0: Prioritizing data security to tackle frauds in digital lending industry' (ET, 24 January 2024) <https://ciso.economictimes.indiatimes.com/news/cyber-crime-fraud/cybersecurity-2-0-prioritizing-data-security-to-tackle-frauds-in-digital-lending-industry/107109298> accessed 31 July 2024.
42. 'A Smarter Approach to Risk Management' (LexisNexis) <https://risk.lexisnexis.com/global/en/products/threatmetrix> accessed 31 July 2024.
43. 'A Smarter Approach to Risk Management' (LexisNexis) <https://risk.lexisnexis.com/global/en/products/threatmetrix> accessed 31 July 2024.
44. Customer Data Monitoring Solution' (LexisNexis) <https://risk.lexisnexis.com/corporations-and-non-profits/customer-information-management/customer-monitoring> accessed 31 July 2024.
45. 'A Smarter Approach to Risk Management' (LexisNexis) <https://risk.lexisnexis.com/global/en/products/threatmetrix> accessed 31 July 2024.
46. 'Actionable Intelligence from Human Interactions' (LexisNexis) <https://risk.lexisnexis.com/global/en/products/behaviosec> accessed 31 July 2024.
47. 'Actionable Intelligence from Human Interactions' (LexisNexis) <https://risk.lexisnexis.com/global/en/products/behaviosec> accessed 31 July 2024.

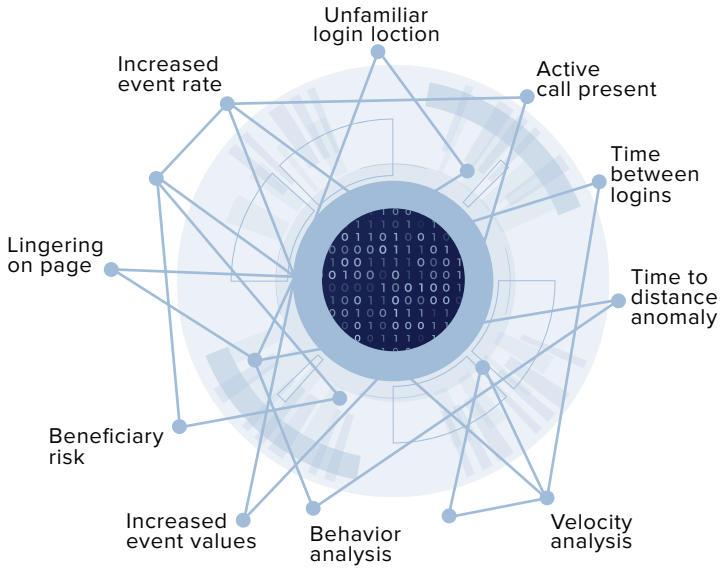


Figure 5: Technological solutions can leverage AI to accelerate risk-based decisions with an automated, precise risk score.[48]

Technological solutions can rely on AI to accelerate risk-based decisions. These AI-based solutions often rely on several factors to identify suspicious activity on an account and flag the same. These factors include the following:

a. **Increased event rate:** It monitors a sudden increase in user activity which may suggest automated or suspicious activity through this account.
b. **Lingering on page:** Tracks the user activity on the page such as unusually long pauses which may indicate fraudulent intent or hesitation.
c. **Increased event value:** Flagging unusually high transaction amount, which may indicate that the account is compromised and is being used for unlawful activities.
d. **Behaviour analysis:** It examines user behaviour patterns to highlight unusual behaviour. It looks for deviations from the usual approach/pattern of the user, which might indicate that the account is compromised.
e. **Active call present:** It informs if a call is active during the transaction, indicating potential social engineering attempt.
f. **Time between logins:** These solutions measure the time between consecutive logins to gain insight on the user behaviour and then observe the account for any suspicious activity.
g. **Unfamiliar login location:** They monitor if the user logs in from an unexpected or unusual location, indicating unauthorised usage of the account.
h. **Time to distance anomaly:** This means time taken to log in from different locations suggesting that the account might be compromised.
i. **Velocity analysis:** It scrutinises the speed of the transaction, wherein rapid actions can suggest that an automation technique is being used by the criminal.
j. **Beneficiary risk:** To assess the risk associated with the recipient of the transaction which can indicate that the account might be used for fraudulent activities.

By evaluating these factors, a technological solution provider can assess the chances of fraudulent activity, which further enables the organisation to make informed decisions to prevent fraudulent activity.

For instance, if a user suddenly requests a large loan from a new device or location, the system can flag it as suspicious and require additional verification. Advanced authentication methods, like biometric verification and out-of-band authentication, can significantly reduce the risk of social engineering scams.[49]

48. 'A Smarter Approach to Risk Management' (LexisNexis) <https://risk.lexisnexis.com/global/en/products/threatmetrix> accessed 31 July 2024.
49. 'One Time Password' (LexisNexis) <https://risk.lexisnexis.com/global/en/products/one-time-password#:~:text=Authenticate%20a%20user%20with%20a,value%20transaction%20with%20a%20customer> accessed 31 July 2024.

AI-driven solutions can analyse various factors, such as typing patterns and facial recognition, to verify the user's identity, offering higher security levels than traditional passwords and PINs.[50] Additionally, these systems can provide real-time threat detection by evaluating multiple data points simultaneously, enabling digital lending platforms to identify and respond to potential social engineering scams instantly.

3.3. Security Breaches

3.3.1. Reasons for Concerns

As fintech companies increasingly adopt cloud services to store their data, significant risks are attached to this shift. Attackers can exploit weaknesses in the service provider's cloud configurations and security settings, gaining unauthorised access to sensitive information. Moreover, the growing adoption of fintech solutions has increased interconnected devices and Application Programming Interfaces (APIs) within fintech ecosystems.

This expansion ultimately broadens the attack surface for cybercriminals, providing them with more opportunities to find and exploit vulnerabilities within the system. By exploiting these weak points, cybercriminals can infiltrate fintech networks, deploy ransomware, encrypt critical data, halt company operations, and demand payment for the data's release.[51]

3.3.2. Possible Solutions

Digital lending companies can address security breaches by employing real-time solutions that identify suspicious changes and misconfigurations. Technological solutions, such as advanced file integrity monitoring (FIM) and security configuration management (SCM), offer robust protection by providing real-time detection of security issues.[52] Leveraging these technologies can solutions can enhance threat detection and safeguard against unauthorised access and security breaches.

Overall, a multifaceted approach is necessary to tackle challenges within the digital lending ecosystem. First, app marketplaces and social media platforms may need to implement stricter policies and enhanced monitoring to combat unauthorised lending apps. Second, for social engineering scams, advanced technological solutions, including sophisticated authentication mechanisms and real-time monitoring, can address social engineering scams. Lastly, for security breaches, robust real-time detection systems are important. By adopting these advanced technologies and strengthening existing solutions, digital lending companies can effectively manage and mitigate these risks.

50. 'One Time Password' (LexisNexis) <https://risk.lexisnexis.com/global/en/products/one-time-password#:~:text=Authenticate%20a%20user%20with%20a,value%20transaction%20with%20a%20customer> accessed 31 July 2024.
51. 'PWC, Beyond the cloud: Navigating FinTech cyber threats and fortifying defences (PWC, 2024) <https://www.pwc.in/assets/pdfs/consulting/beyond-the-cloud-navigating-fintech-cyber-threats-and-fortifying-defences-v3.pdf> accessed 05 August 2024
52. 'Fortra's Tripwire Enterprise', (Tripwire) <https://www.tripwire.com/offers/tripwire-enterprise?utm_source=google&utm_medium=cpc&utm_campaign=apac&utm_term=india&_bt=694771368391&_bk=cyber%20security%20tech%20companies&_bm=p&_bn=g&_bg=161903918844&gad_source=1&gclid=Cj0KCQjw8MG1BhCoARIsAHxSiQn5UMfVrCoqZiTEKeCfzSgCjbTSRrjGbIAjR_Ug2cwo4RYGOI9WTQwaAudsEALw_wcB> accessed on 06 August 2024

4 Potential Reasons For Low Adoption of Technological Solutions

In the digital lending ecosystem, concerns about security and the availability of technological solutions have been present for some time. However, the adoption of these technologies remains limited. In this chapter, we will explore why digital lending companies have been hesitant in embracing these solutions despite their potential to enhance security. The factors contributing to this low adoption rate are detailed below.

4.1. Disproportionate reliance on in-house capacities

Many digital lending platforms disproportionately rely on their in-house teams to develop and maintain technological solutions.[53] While this approach can provide advantages such as customised solutions that meet specific business needs, it often limits the adoption of advanced, state-of-the-art technologies. In-house teams may often lack the specialised expertise required to effectively implement and integrate complex technological solutions. Over-reliance on internal resources can slow innovation and hinder the company's ability to keep pace with the rapidly evolving technological landscape.

4.2. Limited awareness of technological solutions

A major barrier to adopting technological solutions in digital lending is the limited awareness among stakeholders about the available technologies and their potential benefits. Many digital lending companies may not be fully informed about cutting-edge solutions, such as artificial intelligence and machine learning, which can enhance operations, improve security, and streamline processes. This knowledge gap can lead to reluctance in investing in new technologies, as decision-makers may not fully grasp the return on investment or the competitive advantages these technologies can offer.

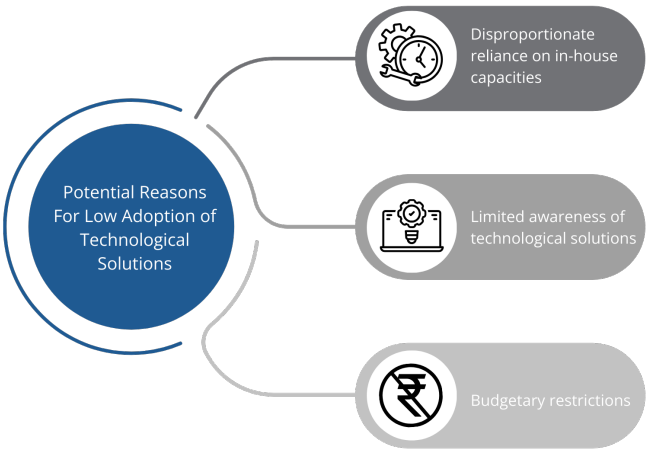


Figure 6: Potential Reasons For Low Adoption of Technological Solutions

[53] 'Event Report- Conference on Customer Protection in Digital Lending: Way Forward' (The Dialogue, 6 May 2024) <https://thedialogue.co/-publication/event-report-conference-on-customer-protection-in-digital-lending-way-forward/#:~:text=The%20inaugural%20stakeholder%20consultation%20took,insights%20on%20the%20identified%20themes> accessed 31 July 2024.

4.3. Budgetary restrictions

Budgetary restrictions are a critical factor hindering the adoption of advanced technological solutions. Implementing new technologies often requires substantial financial investment, including costs for purchasing software and hardware, training staff, and integrating these solutions into existing systems. Smaller digital lending platforms, in particular, may struggle to allocate sufficient funds for these purposes. Even larger firms might face financial constraints that lead them to prioritise other business needs over technological upgrades, resulting in a slower adoption rate.

5 Way Forward

The Indian digital lending sector has experienced significant growth alongside increasing challenges, such as the rise in unauthorised lending apps, social engineering scams, and cybersecurity concerns. The following recommendations are proposed for various stakeholders, including the government, security solution providers, digital lending companies, and the broader ecosystem to address these issues.

5.1. Recommendations for the Government

The challenges in the Indian digital lending sector require a comprehensive approach that complements the existing policy frameworks. To address the proliferation of unauthorised lending apps, social engineering scams, and security breaches, the following multifaceted approach is recommended:

5.1.1. Tackling the Proliferation of Unauthorised Apps

The RBI's Digital Lending Guidelines (DLG), introduced in September 2022[54] aim to regulate digital lending practices and protect consumers.[55] Additionally, the RBI is considering the establishment of the Digital India Trust Agency (DIGITA) to combat unauthorised lending apps. DIGITA would verify digital lending apps and maintain a public register of verified apps.

Apps lacking DIGITA's 'verified' signature would be deemed unauthorised for law enforcement purposes, serving as a crucial checkpoint against financial crimes in the digital realm.[56] The RBI also engages with app marketplaces to take down apps against which complaints are received.[57] It is important that the DIGITA framework is proactively pursued by incorporating the perspectives of all stakeholders.

Figure 7: Key Stakeholders in the Discourse

54. 'Digital Lending Guidelines' (RBI, 14 February 2023) <https://www.rbi.org.in/commonperson/english/scripts/FAQs.aspx?Id=3413#:~:text=Ans%3A%20The%20Guidelines%20are%20applicable,on%20Guidelines%20on%20Digital%20Lending> accessed 30 July 2024.
55. 'Guidelines on Digital Lending' (RBI, 2 September 2022) <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/GUIDELINESDIGITALLENDINGD5C35A71D8124A0E92AEB940A7D25BB3.PDF> accessed 30 July 2024.
56. 'RBI to set up Digital India Trust Agency to check illegal lending apps' (Business Standard, 31 March 2024) <https://www.business-standard.com/finance/news/rbi-to-set-up-digital-india-trust-agency-to-check-illegal-lending-apps-124033100152_1.html> accessed 30 July 2024.
57. 'Google removes 2,200 fraudulent loan apps from Play Store: MoS Finance' (Hindustan Times, 06 February 2024) <https://www.hindustantimes.com/technology/google-removes-2-200-fraudulent-loan-apps-from-play-store-mos-finance-101707215359684.html> accessed 04 Augsut 2024

In addition to these measures, establishing a Self-Regulatory Organisation (SRO) within the digital lending industry could further enhance the implementation of regulations. An SRO would promote dialogue between the government and industry stakeholders, helping to refine and enforce the whitelisting framework. This organisation could set industry standards and best practices, work alongside regulatory bodies to ensure compliance and address industry-specific challenges, fostering a culture of self-regulation and accountability.[58]

5.1.2. Tackling Security Breaches

The Information Technology Act of 2000 (IT Act) forms the basis of cyber security protection in India. Furthermore, the recently introduced Digital Personal Data Protection Act (DPDPA) has outlined vital data handling principles, including obtaining explicit consent, limiting data to specific purposes, ensuring data accuracy, implementing robust security measures to prevent unauthorised access, and promoting transparency and accountability in data practices. Organisations can restrict access to financial information, employee information, business plans and client details to a few employees. Organisations must also subscribe to up-to-date protection tools to block malicious sites. Rule 8 of SPDI Rules, 2011 requires body corporates to adhere to the IS/ISO/IEC 270001 standard.

To complement these frameworks, tailored cybersecurity guidelines may be needed for the fintech sector, as the national cybersecurity guidelines last came out in 2013. These separate cyber security guidelines can guide entities to adhere to a set standard of cyber security practices. Further, even though the IT Act has been amended in the past, an overhaul of the law, in light of modern, sophisticated cybersecurity challenges, may be required.

5.1.3. Tackling Social Engineering

The policy changes recommended in the previous part are also relevant to tackling social engineering scams. Further, the government could encourage the growth of startups and companies with cutting-edge technological solutions that can help prevent social engineering, like the ones we discussed in the paper.

The RBI has already created "Regulatory Sandbox: Fourth Cohort on 'Prevention and Mitigation of Financial Frauds' – Exit".[59] Through this regulatory sandbox, the companies could test their products, which included solutions such as a real-time monitoring system. Such regulatory sandboxes aim to bring innovation to financial services by allowing businesses to live-test their solutions in a controlled regulatory environment. Therefore, various government stakeholders could ensure that sandboxes focus on novel technologies that can enhance security in the digital lending space. An alignment in this direction could prove helpful.

Furthermore, to empower digital lending companies, the government can establish knowledge-sharing mechanisms and provide targeted mentoring. Through a comprehensive mentoring facility, the government can assist digital lending companies in understanding aspects such as cybersecurity, social engineering scams, fraudulent methods in the digital lending sector, and innovative technologies available to the ecosystem.

5.2. Recommendations For Solution Providers

Technological solution providers should prioritise developing effective and innovative methods to inform relevant stakeholders, including digital lending companies, about the latest advancements in AI and

58. 'RBI releases finalised framework for Indian fintech sector's self-regulatory body' (Economic Times, 30 May 2024) <https://economic-times.indiatimes.com/news/economy/policy/r-bi-releases-finalised-framework-for-indian-fintech-sectors-self-regulatory-body/articleshow/110561450.cms?from=mdr> accessed 30 July 2024.

59. 'Regulatory Sandbox: Fourth Cohort on 'Prevention and Mitigation of Financial Frauds' – Exit' (Reserve Bank of India, 18 June 2024) <https://www.taxsutra.com/sites/default/files/lsi-news-pdf/-Regulatory%20Sandbox%20Fourth%20Cohort%20on%20%E2%80%98Prevention%20and%20Mitigation%20of%20Financial%20Frauds%E2%80%99%20%E2%80%93%20Exit.pdf > accessed on 20 August 2024

ML-driven analytics and real-time threat detection. Ensuring stakeholders are aware of these advancements will help enhance their security measures.

Additionally, developing solutions that can be customised to complement existing in-house capacities will allow digital lending platforms to improve their security infrastructure without disrupting their operations. Given that cost can be a barrier to adoption, technological solution providers should also consider creating innovative and flexible pricing models. These models should accommodate a range of players, from small startups to large enterprises, to ensure that security solutions are both accessible and scalable across the industry.

5.3. Recommendations for Digital Lending Companies

5.3.1. Combine In-House Capacities and Third-Party Solutions

Instead of relying solely on their internal capacities, digital lending companies should develop strategies that integrate their in-house capabilities with third-party solutions to enhance security measures. This approach can improve their ability to identify and address emerging threats more effectively.

5.3.2. Shift to a Customer-Centric Approach

Ultimately, shifting from a compliance-centric approach to a customer security-centric approach is essential. While adhering to regulations is important, prioritising genuine customer protection can significantly enhance trust and satisfaction. Given the recent challenges in the digital lending sector and existing concerns, focussing on building trust with customers is imperative. Embracing a customer-centric approach can benefit digital lending companies by fostering greater user confidence and loyalty.

5.4. Recommendations for the Ecosystem

5.4.1. Multi-Stakeholder Consultations

Continuous stakeholder consultation will benefit India's digital lending sector. Regular dialogue among government bodies, the digital lending industry, technology solution providers, and civil society can foster a cohesive and effective regulatory environment. Civil society organisations can play the crucial role of bringing stakeholders together in this context. This collaboration can help develop comprehensive policies that address current challenges and anticipate future threats.

For instance, recently, the Hon'ble Finance Minister, along with the RBI, engaged with the fintech sector, where stakeholders emphasised the importance of monthly virtual meetings with regulators to address the concerns faced by fintech startups. Additionally, The Dialogue and DLAI collaborated to conduct two stakeholder consultations, which helped identify problems and brainstorm solutions. Therefore, maintaining a continued consultation process within the digital lending ecosystem can significantly enhance sector-wide customer protection measures.

5.4.2. Public Awareness

Ultimately, educating consumers about the risks associated with digital lending and the importance of cybersecurity is crucial. Civil society stakeholders, especially grassroots organisations and consumer bodies, can play an important role here. Public awareness can significantly reduce the incidence of customers falling victim to scams and illegal lending apps. Consumers should be encouraged to verify the legitimacy of lending platforms and adopt safe online practices. For example, the RBI has launched a Nationwide Intensive Awareness Campaign[60] to promote customer financial literacy and awareness.

The campaign aims to inform customers about their rights and the available complaint redressal

[60] 'Nationwide Intensive Awareness Campaign' (Standard Chartered) <https://www.sc.com/in/important-information/nationwide-intensive-awareness-campaign/> accessed 30 July 2024.

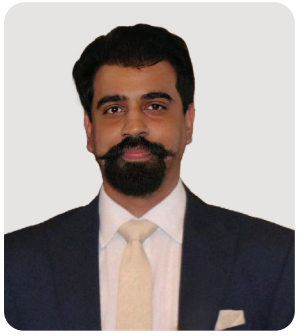
mechanisms, including the Internal Grievances Redress (IGR) and the RBI's Alternative Grievance Redress (AGR) mechanism. Additionally, Fintech Suraksha (FTS), an initiative of DLAI, educates customers on identifying fake or unauthorised lending apps. It emphasises the importance of multi-factor authentication, promotes safety practices while using payment services, and enhances customer knowledge on how to report online financial fraud.[61]

Therefore, addressing the multifaceted challenges in the digital lending industry requires a coordinated effort that integrates technological advancements, regulatory innovations, user awareness, and collaborative governance. By fostering a secure and transparent digital lending ecosystem, we can ensure the sustainable growth of this vital sector while safeguarding consumer interests.

61. 'Fintech association launches awareness campaign about cyber fraud' (Business Standard, 26 January 2024) <https://www.business-standard.com/finance/news/fintech-suraksha-dlai-s-initiative-to-raise-awareness-about-cyber-frauds-124012600637_1.html> accessed 30 July 2024.

Reflections

This white paper highlights Cybersecurity concerns such as social engineering scams, unauthorised lending apps, and security breaches in the Indian digital lending sector. To address these concerns, various stakeholders, including civil society, industry, and the government, must brainstorm solutions together. The white paper marks an essential step in this direction, hopefully catalysing further collaboration within the ecosystem.



Mr. Kazim Rizvi
Founding Director, The Dialogue

The fastest-growing segment of fintech is digital lending, which involves customer data and capital. Consequently, the segment is a natural target for data heists, digital forgeries, and cyberattacks. This report concisely suggests a path forward and a few practical action points to confront the obstacles presented by unauthorised lending app operators, scammers, and cyberthugs. I am confident that the insights gained from this report will be beneficial in resolving these obstacles in a practical manner.

Mr. Jatinder Handoo
CEO, DLAI

This informative white paper sheds light on crucial cybersecurity concerns, including social engineering attacks which exploit the human element. Many authentication methods rely heavily on static data, which is inefficient when attackers are constantly evolving their attacks. Hence, as identified in the paper, we must move beyond traditional authentication and embrace multi-factor authentication and behavioural biometrics to combat social engineering. At the same time, we should remain cognizant of balancing risk mitigation with a positive customer experience.

Mr. Cameron Church
Director, Market Planning - Fraud & Identity,
LexisNexis® Risk Solutions

This comprehensive white paper by DLAI and The Dialogue is a timely contribution to the digital lending landscape. The emphasis on curbing unauthorised lending apps and fortifying security measures through policy frameworks is not only prudent but also highly pertinent at this juncture. The white paper's analysis highlights the urgent need for all stakeholders to collaborate on creating a more secure and transparent digital lending ecosystem.

Mr. Manish Lunia
Cofounder, FlexiLoans

As we navigate the challenges of digital lending, the white paper offers a clear and actionable roadmap for enhancing customer protection. The in-depth analysis of security breaches and the need for real-time detection solutions resonates strongly with our commitment to safeguarding customer data. This document will guide us in implementing robust security practices that align with industry standards.

Mr. Anuj Kacker
Cofounder, Freo

The DLAI & The Dialogue white paper on Customer Protection in the Digital Lending Ecosystem in India is a timely and invaluable resource for our industry. The paper's deep dive into Cybersecurity concerns, including unauthorised lending apps, social engineering scams, and data breaches, throws light on some of the challenges the fintech industry faces. The recommendations, such as leveraging a combination of in-house capabilities and third-party technological solutions, are critical for creating a secure and trustworthy digital lending environment for our customers.

Mr. Sanjay Aggarwal
Cofounder, Moneyview

The DLAI & The Dialogue white paper meticulously addresses the pressing Cybersecurity concerns in digital lending, from the proliferation of unauthorised apps to the growing threat of social engineering scams. The proposed solutions, including enhanced monitoring and public awareness campaigns, are critical steps toward rebuilding consumer trust and ensuring the sustainable growth of our industry.

Ms Shaili Maheshwari Kajaria
Cofounder, Tezz Capital

The insights provided in the white paper are indispensable for any digital lending firm. The recommendations for shifting to a customer-centric approach and adopting advanced technological solutions reflect the evolving needs of our sector.

Mr. Shivashish Chatterjee
Co-Founder, DMI Finance

thedialogue.co

@_DialogueIndia

@TheDialogue_Official

@The-Dialogue-India

@TheDialogueIndia

dlai.in

@dlai_india

@dlai_india

@Digital Lenders Association of India (DLAI)

@dlai