



# The Dark Side of the Chinese Loan Applications



This exposé by Ij-Reportika uncovers the unsettling realities concealed beneath the seemingly innocuous facade of digital lending.



## Table of Contents

<b>The Dark Side of the Chinese Loan Applications</b> .....	2
<b>Exploiting Personal Data for Extortion and Illicit Profits</b> .....	3
<b>Tactics Employed by Chinese Loan Apps “Agents”</b> .....	4
<b>Unnecessary Permissions to Harass Users</b> .....	5
<b>The Alternate Routes to Reach People</b> .....	8
<b>Countries Case Studies</b> .....	10
<b>Phillippines</b> .....	10
<b>IJ-Reportika Survey</b> .....	14
<b>India</b> .....	15
<b>IJ-Reportika Survey</b> .....	19
<b>Pakistan</b> .....	20
<b>IJ-Reportika Survey</b> .....	23
<b>Africa</b> .....	24
<b>IJ-Reportika Survey</b> .....	30
<b>Protective Measures Against Chinese Loan App Scams</b> .....	32
<b>Conclusion</b> .....	32
<b>References</b> .....	34

## The Dark Side of the Chinese Loan Applications

Embarking on a journey into the shadows, our investigative report delves deep into the intricate web of Chinese Loan Applications, revealing a disconcerting narrative that extends beyond borders. Titled "**The Dark Side of Chinese Loan Applications**," this exposé uncovers the unsettling realities concealed beneath the seemingly innocuous facade of **digital lending**.

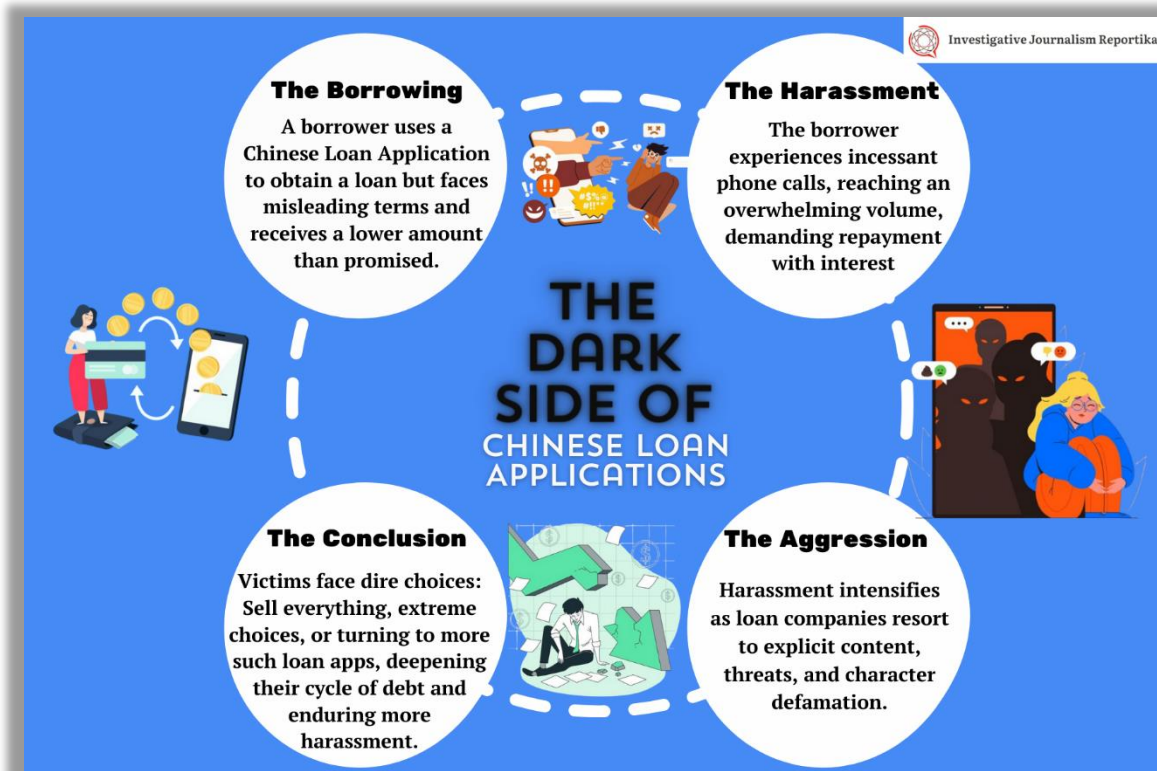


Figure 1 The Vicious Cycle of the Chinese Loan Apps

From countries in **South Asia, South East Asia** to the intricate landscapes of **Africa**, our exploration unveils stories of individuals caught in a merciless cycle of **exploitation, harassment, and economic upheaval**. As we traverse through the underbelly of this pervasive issue, the report sheds light on the **personal ordeals** and **systemic threats** that mark the dark side of Chinese loan apps. Join us on this journey to unravel the hidden dimensions and consequences of the ever-expanding influence of these applications.

## Exploiting Personal Data for Extortion and Illicit Profits

In our investigation, a stark revelation emerged regarding the **intrusive nature** of Chinese Loan Applications, which not only **exploit financial vulnerabilities** but also brazenly invade **personal privacy**. These applications, under the guise of loan processing, surreptitiously access sensitive data, including **contact books and gallery permissions**. Shockingly, our findings indicate that this personal information becomes a potent tool for malicious purposes.

In instances involving **female victims**, loan providers resort to despicable acts of **blackmail**, threatening to **disseminate morphed images to their contacts**. Beyond such heinous practices, our investigation indicates a disturbing trend – the sale of this **pilfered personal data on online platforms and the dark web**. The consequences are far-reaching, ranging from the inundation of contacts with various **advertisements** to the orchestration of targeted advertising campaigns. This blatant disregard for **individuals' privacy** underscores the insidious nature of these applications and amplifies the urgent need for regulatory intervention.



Figure 2 Exploitation of Victims using Fake Loan Agreements

## Tactics Employed by Chinese Loan Apps “Agents”

1. **Relentless Calls from Loan Recovery Agents:** These agents, oblivious to decency, persistently hound borrowers throughout the day, indifferent to appropriate timing and even encroaching into the late hours of the night. The incessant calls become a source of perpetual worry and disruption for the already distressed borrower.
2. **Verbal Assault and Menacing Language:** The lenders stoop to the lowest depths by employing abusive language and delivering explicit threats during their relentless calls. The borrower is subjected to a barrage of intimidating messages, including threats of physical harm to themselves or their loved ones if they fail to meet the stringent repayment terms.
3. **Exploitative Blackmail Tactics:** Resorting to blackmail, lenders exploit the vulnerability of borrowers by threatening to divulge sensitive personal information or initiate legal action against them.

In numerous countries, loan providers engage in the reprehensible practice of **harassing female victims** by creating morphed images and subsequently blackmailing them with threats of exposing these images to their friends and family.

4. **Intrusive Harassment of Contacts:** Loan providers, armed with access to the borrower's contacts, extend their harassment to friends, family, and employers. The borrower, now subjected to humiliation on multiple fronts, grapples with the profound distress caused by this intrusive violation of privacy.
5. **Menacing Messages Delivered Across Platforms:** The lenders escalate their torment by bombarding the borrower's phone and email with threatening messages. In an insidious move, they extend their reach to the borrower's social media accounts, posting menacing messages that further intensify the psychological toll on the victim.



## Unnecessary Permissions to Harass Users

Our investigation has revealed that certain loan applications engage in concerning practices where **unnecessary permissions are requested from users**. According to our investigation, beyond the legitimate requirements for loan processing, these applications exploit their users by seeking access to sensitive information such as **personal contacts, pictures, and location data**. This unwarranted intrusion not only poses a **serious breach of privacy** but also creates a platform for **harassment, tracking, and intimidation**.

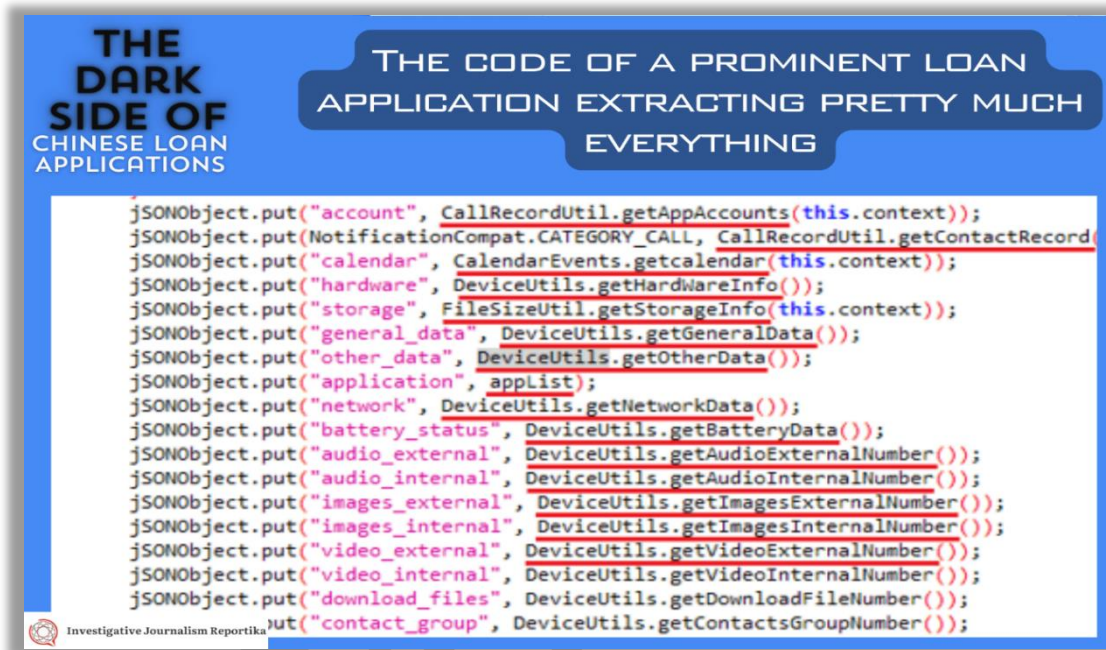


Figure 3 The Code of a Loan Application Extracting Unnecessary Data

A compelling case study delves into the operations of the widely-used loan application in the **Philippines, Atome PH**. Notably, two-thirds of the individuals managing its Facebook Page hail from **China and Taiwan**. However, user experiences with the application reveal a troubling pattern—many have voiced concerns about the app's **abrasive treatment during repayment, subpar customer support, and the imposition of undisclosed charges**.

This application, available on both Google Playstore and App Monk, demands a considerable array of **permissions**, including access to the **camera device, network sockets, external storage, user contacts, calendar data, account lists, and even location details**. This level of data access raises significant privacy and security concerns for users, prompting a closer examination of the practices employed by Atome PH.

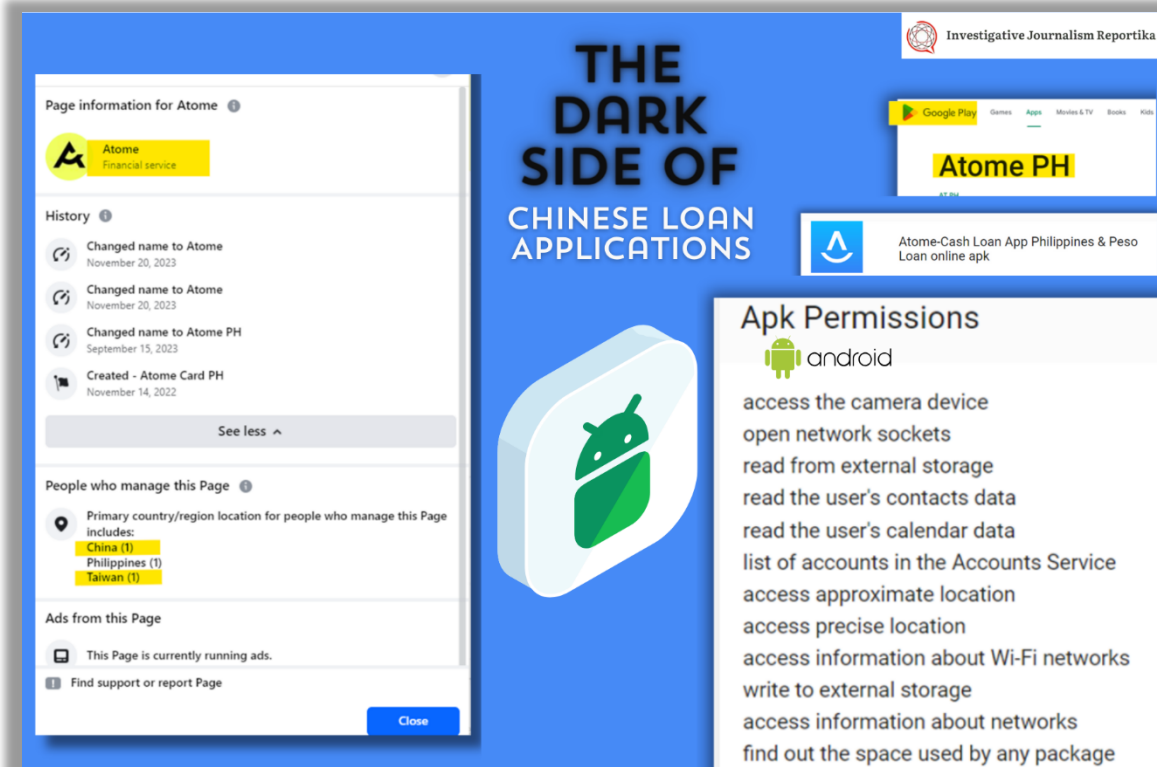


Figure 4 Case Study of the Atome PH Application

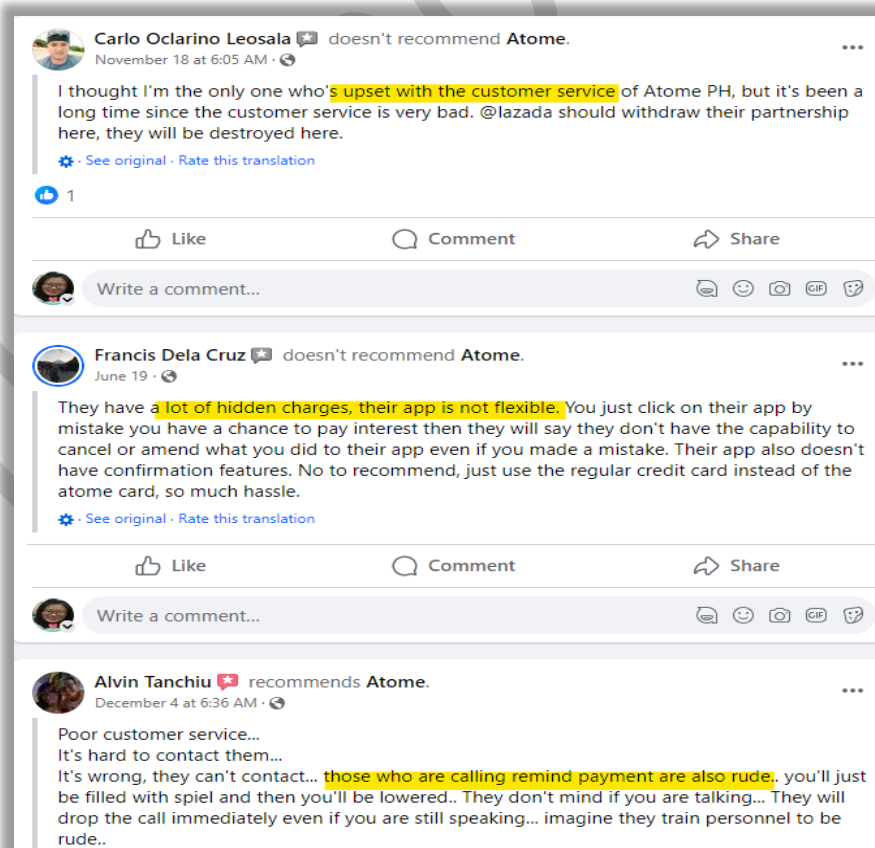


Figure 5 The Users Calling out the Scam of Atome PH Lending App

**Atome-Cash Loan App Philippines & Peso Loan online apk**

Updated On: Mar 16, 2020 | App Version: 1.5.1

[DOWNLOAD APK](#)

This apk is safe to download from this mirror and free of any virus.

[Check Previous Versions](#)

Showcase your Android App on apkmonk [Submit App](#)

**App Info**

App Download Version	1.5.1
Last Updated	Mar 16, 2020
Apk Size	11M
App by	Atome PH
Category	Free Finance App
Content Rating	Everyone
Support Android Version	Android 19 and above
App Package	ph.kreditpintar
Get it on	Google Play

Figure 6 Atome PH Lending App

In another case study examining the **Mr.Cash application**, our investigation has uncovered alarming findings that highlight a troubling trend of predatory lending practices and potential privacy violations. Our investigation delves into the questionable practices surrounding the **Mr.Cash application**, a lending platform promoted through the Facebook group "**Cash PH Loan**," boasting over **6.8K active members**.



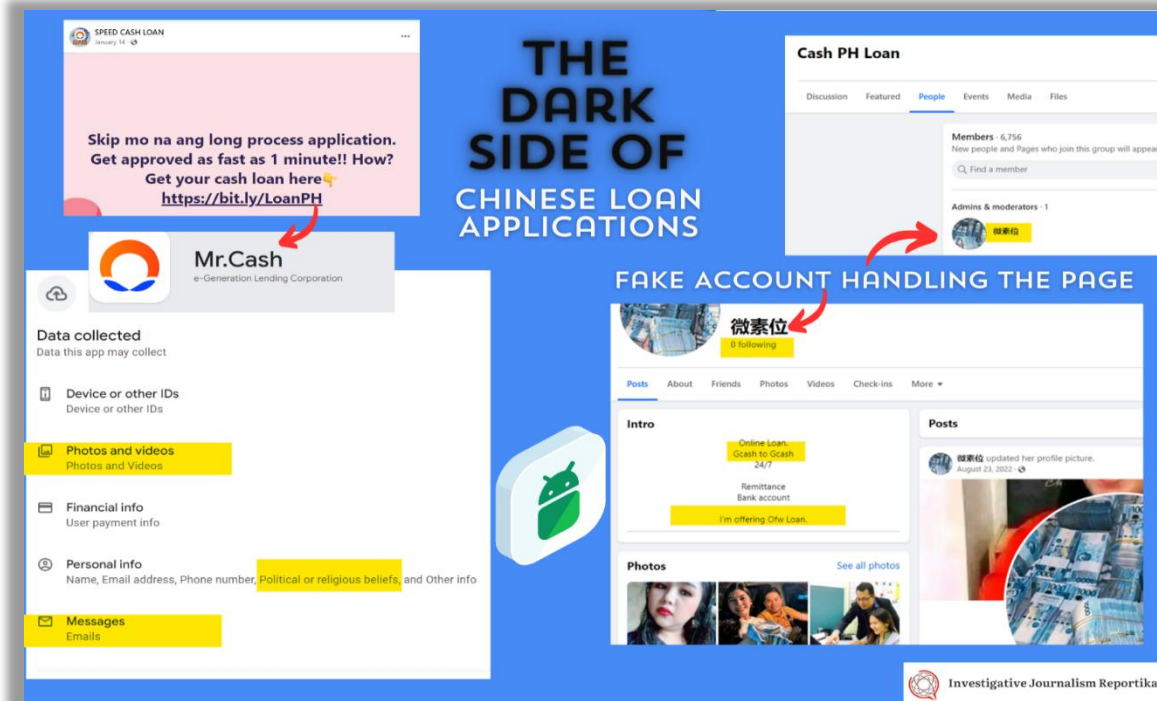


Figure 7 Case Study of the Mr Cash Lending App

Through a combination of **online scrutiny and interviews with multiple users of the application**, a disconcerting pattern of discontent and potential misconduct has emerged. Users within the group have reported a range of issues, from exorbitant interest rates to aggressive collection methods, creating an atmosphere of unease and dissatisfaction. Furthermore, the group's administrator, identified as **微素位**, adds an air of suspicion, with the **lack of transparent information amplifying concerns**. In our interviews, users raised alarm over the extensive permissions requested by **Mr.Cash**, like of **personal photos and videos** for security and compliance purposes.

### The Alternate Routes to Reach People

In response to mounting complaints from countries such as India and the Philippines, Google Play Store and Apple App Store have taken significant steps to address concerns related to **predatory lending practices** by removing a substantial number of Chinese loan applications from their platforms. Despite these efforts, a concerning number of such applications still persist, perpetuating exploitative practices that have drawn widespread criticism. Moreover, beyond the purview of mainstream app stores, numerous unregulated or less prominent platforms such as **Apptimizer, CNET, Softonic, APKMirror, APKPure, Aptoide, Uptodown, APKCombo, and AndroidAPKsFree** continue to host and distribute these problematic applications, thereby enabling them to target and exploit millions of users.

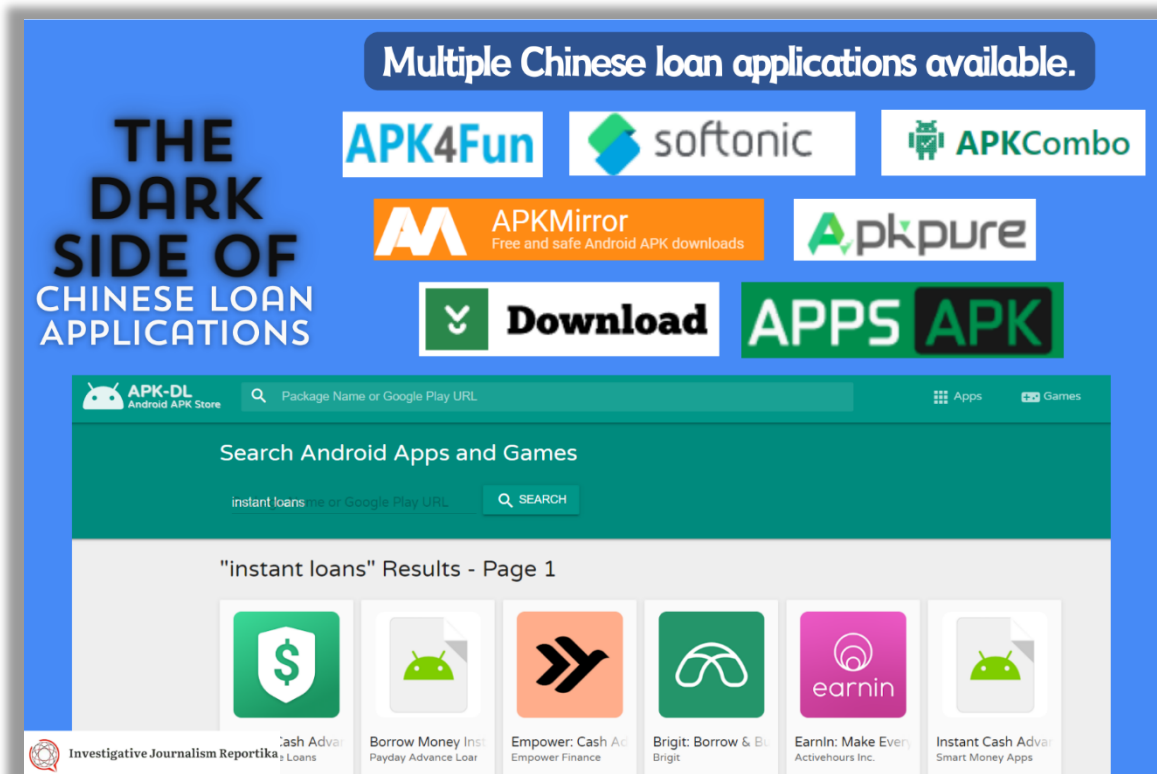


Figure 8 App Stores other than Google Playstore

In numerous countries, a concerning trend involves the distribution of APKs for banned or unapproved applications directly to users through platforms like **TikTok, Facebook and WhatsApp**. This method circumvents official app stores' restrictions, potentially exposing users to security and privacy risks associated with sideloading unauthorized applications.

## Countries Case Studies

### Philippines

The Chinese loan app scams in the Philippines are a form of online fraud that targets vulnerable borrowers who need quick cash. These scams involve **unlicensed and unregulated lending apps** that offer **high-interest loans** with **short repayment periods**. The borrowers are required to give access to their contacts, cameras, and social media accounts as part of the loan terms and conditions. If they fail to pay on time, the **lenders harass and threaten them** and their contacts with **abusive messages, calls, and even blackmail**. Some of the victims are also tricked into downloading more apps that increase their debts.

From January to November 2023, our investigation unveiled the amassing of more than **12 Million Peso**. This money funnelled into the accounts of cybercriminals utilizing over **90 malicious Android apps to dupe their targets**.

The Philippine authorities have been cracking down on these illegal lending apps and their operators. In **February 2022**, the **Philippine National Police - Anti-Cybercrime Group (PNP-ACG)** arrested 46 suspects, including a Chinese national, who were behind several lending apps that scammed thousands of Filipinos. The suspects were charged with violation of the **Cybercrime Prevention Act of 2012**.

The **Securities and Exchange Commission (SEC)** also **banned 19 lending apps** that were operating without a certificate of authority or license in the Philippines. The SEC warned the public to be cautious and to take measures before engaging in online transactions to avoid being victims of **online fraud**.

Individuals in urgent need of cash often find themselves falling victim to the deceptive practices associated with **the "120-day" loan term**. The repercussions of this are felt as early as the **7th day**, with **relentless text messages and calls from debt collectors**.

Moreover, the disbursed amounts from these platforms often deviate significantly from the **advertised figures**. For instance, **PeraMoo promotes a loan amount of P25,000, but a closer look reveals that P10,000 is allocated to interest and additional fees**. Consequently, the actual disbursed amount is only **P15,000**. This translates to a staggering **40% in interest** and charges that victims are compelled to pay.

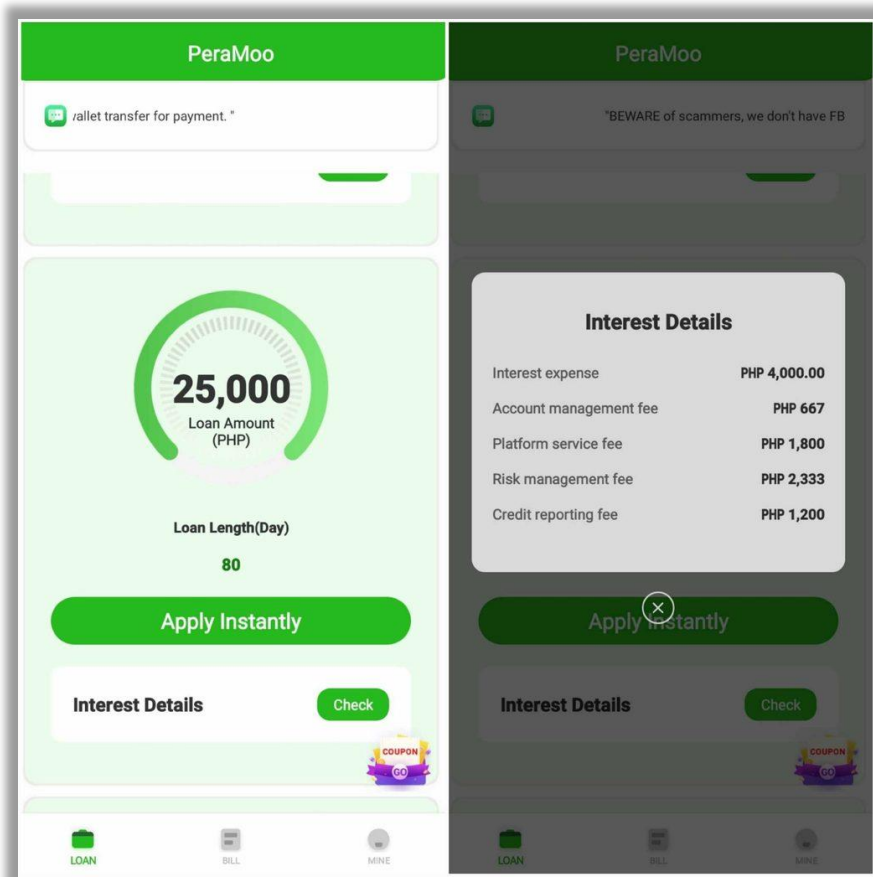


Figure 9 PeraMoo App Interface

The breakdown of these interest and fees includes **P4000** for **interest expenses**, **P2333** for the **risk management fee**, **P1800** for the **platform service fee**, **P1200** for the **credit reporting fee**, and **P667** for the **account management fee**. The disparity between **advertised and actual amounts**, coupled with the **intricate fee structure**, underscores the need for **increased transparency and consumer protection** in the online lending industry.

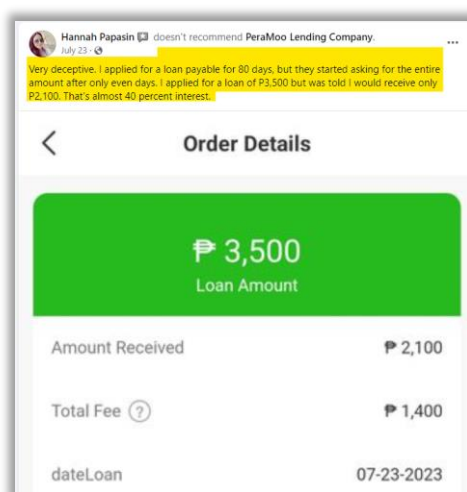


Figure 10 PeraMoo App Fees Breakdown

Several **social media groups** and pages in the Philippines, as shown in the image have been implicated in duping people through **loan scams**. These platforms, despite their seemingly helpful intentions, have been associated with **deceptive practices**, preying on individuals seeking **short-term loans**. It's crucial for users to exercise caution and verify the **legitimacy of these groups**, as they may expose unsuspecting borrowers to potential scams and financial risks.

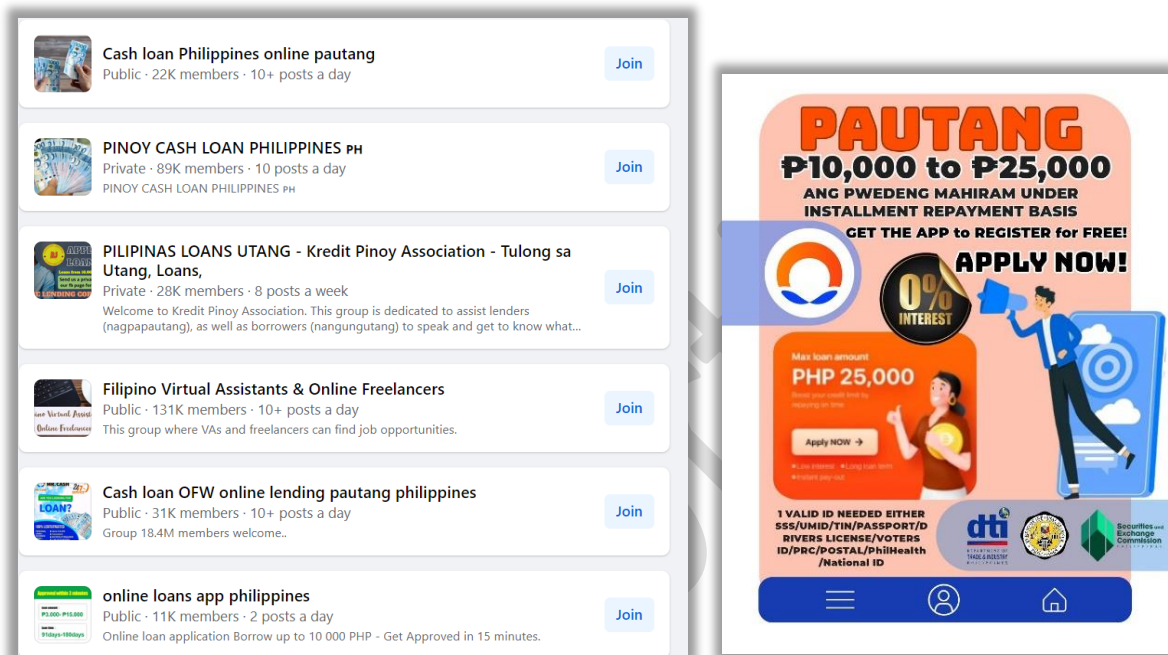


Figure 11 The Philippines Lending Groups

Upon investigation, it has been discovered that a significant number of individuals associated with these groups have **encountered fraudulent activities**. Notably, the managing accounts of these groups are often found to be **fake**. This underscores the importance of exercising extreme caution when engaging with online lending platforms and social media groups offering financial services.



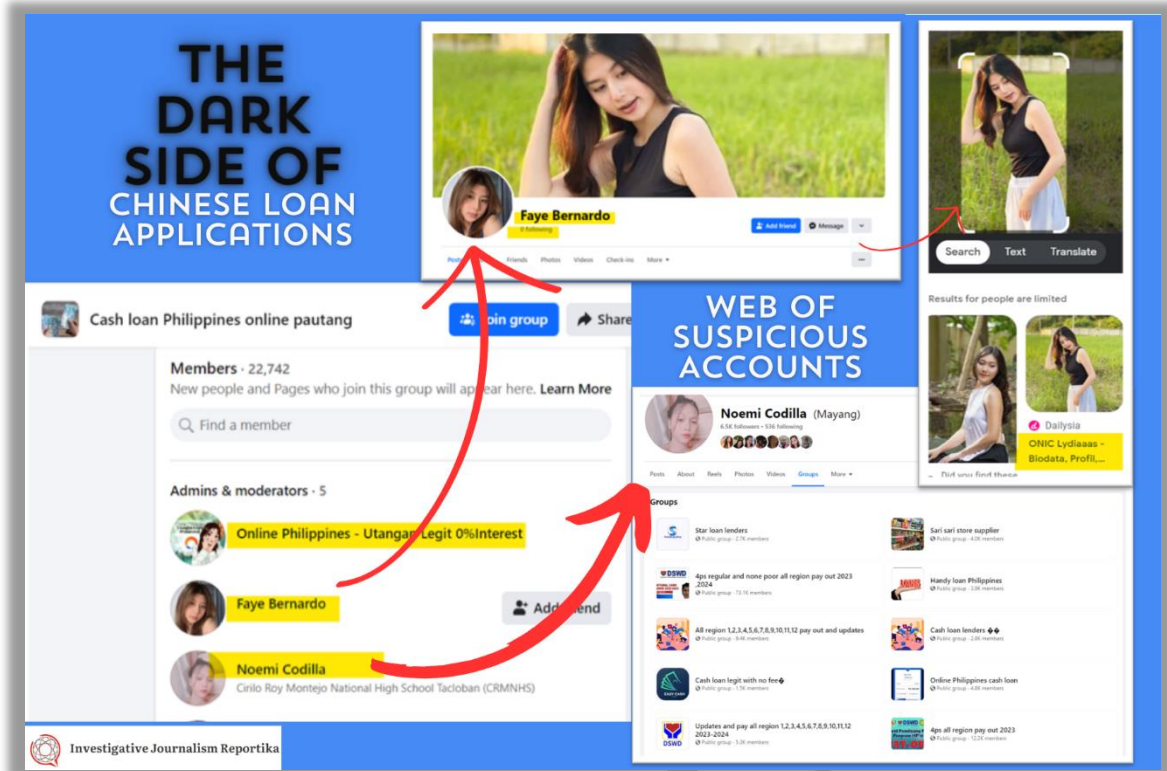


Figure 12 The Dubious Facebook Lending Groups in the Philippines

Filipino users have formed **support groups to combat lending scams**, sharing **experiences** and **raising awareness about deceptive applications**. These communities empower members to exchange information, offer mutual assistance, and collectively **promote financial literacy**. Through shared stories and advocacy, they aim to create a more informed and **vigilant user base**, fostering a safer online lending environment in the Philippines.



Figure 13 The groups raising awareness in the Philippines

In our recent extensive survey conducted by IJ-Reportika in the Philippines, involving a substantial sample size of **100,000 individuals (age group 25-40 years)**, we uncovered significant trends related to the usage of Chinese loan applications. The study spanned four major cities, namely **Manila, Quezon City, Cebu City, and Davao City**.



Figure 14 Ij-Reportika Survey Results in the Philippines

Within this demographic, in 2023, a whopping **790 individuals** admitted to using **Chinese loan applications**, with a notable revelation that a significant portion of these users were lured in through **misleading advertisements on Facebook groups**. Among these users, a substantial **87.97%** (695 individuals out of 790) reported instances of harassment following their interaction with these platforms. Furthermore, **0.89% of respondents** (7 individuals out of 790) disclosed that they personally knew someone within this demographic who had **tragically taken their own life**, attributing the distressing event to the pressures associated with the loan applications.

The survey also highlighted the challenges posed by the proliferation of applications through **non-Google PlayStore app stores, Facebook, and TikTok direct app links**, indicating a pressing need for regulatory measures to control these channels and protect individuals from exploitation and harm in the digital lending landscape in the Philippines.

## India

The rising influence of **Chinese entities in India** poses a **multifaceted threat**, with two prominent facets garnering significant attention. First and foremost is the surge in Chinese lending apps within India, specifically **targeting low-middle-wage citizens**. These applications, capitalizing on economic hardships, entice individuals with the promise of seemingly **attractive loans accompanied by high-interest rates**. This micro-level concern extends to the macroeconomic realm, where Chinese Foreign Direct Investment (FDI) has permeated various sectors, prompting apprehensions regarding economic dependency and national security. Although efforts such as **FDI policy revisions** have been implemented, the challenges persist, presenting a complex landscape at both individual and broader economic levels.

In 2023, our investigation unveiled the amassing of more than **INR 14.3 million**. This money funnelled into the accounts of cybercriminals utilizing over **70 malicious Android apps** to dupe their targets. Our examination exposed more than **22 covert payment gateways** managed by Chinese individuals. These adjustments represent a reaction to heightened legal scrutiny as cybercriminals aim to avoid detection.

The scammers' strategy is surprisingly straightforward:

1. **False Promises:** They create fake instant loan apps that offer substantial loans with flexible repayment terms.
2. **Data Collection:** Victims are deceived into sharing personal details, including name, address, phone number, and bank account information, all in the guise of securing a loan.
3. **Permission Granted:** The malicious app coerces users into allowing access to their contacts and other sensitive data on their mobile devices.
4. **The Loot:** After the victim provides all the requested information and pays the processing fee (usually **5% of the promised loan**), the scammers disappear, leaving the promised loan unrealized.
5. **The Harassment:** In our harrowing investigation, we uncovered the dark reality of certain companies that not only provide loans to users but stoop to the depths of tormenting them, coercing repayment well before the agreed-upon period.

In our investigation, we engaged with an **Indian Chinese Loan Application User**, referred to as Nisha for her safety. Nisha chillingly recounted, "**The loan managers escalated from threats and verbal abuse to using advanced AI to**

**morph my images sourced from social media. They blackmailed me with the threat of leaking these morphed nude/semi-nude pictures.”**

Nisha, summoning courage, eventually confided in her parents and filed a police complaint. These shocking incidents, far from isolated, have pushed numerous individuals to such depths of despair that some tragically opted to end their lives. The documented cases we encountered through Indian media portray a heart-wrenching tableau of this merciless exploitation.

**Some other anecdotes our investigation revealed from India:** Bhoomi of Mumbai, lured by a Chinese Loan Application, borrowed Rs 47,000 in December, promised a 90-day period but received only Rs 40,000 after a supposed processing fee deduction. Relentless calls demanding repayment pushed her to borrow from 60 apps, accumulating a staggering debt of Rs 16 lakh by February. She faced horrifying harassment, with loan companies Plump and ForPay sending morphed pictures to her contacts, escalating to explicit images and threats of prostitution on porn sites.



Figure 15 Tragic Tales of Lending Scams from the Indian Newspapers

In Odisha, Sujay faced similar distress borrowing Rs 1.3 lakh from Kash Loan, enduring accusations of fraud, cheating, and rape sent to his contacts. Ceasing the harassment required a payment of Rs 3.5 lakh.



Tamil Nadu's Selva borrowed Rs 20,000 from Cash World, facing false accusations of heinous crimes circulated among friends, family, and colleagues.

In Gujarat, Bharat Motwani's delayed repayments of Rs 35,000 from Money View, Insta Money, and Flex Salary resulted in obscene, morphed photos sent to 231 contacts.

**Police indifference in India has exacerbated the situation**, with these cases being largely overlooked. Additionally, we identified several applications falling into similar categories, contributing to the ongoing challenges.

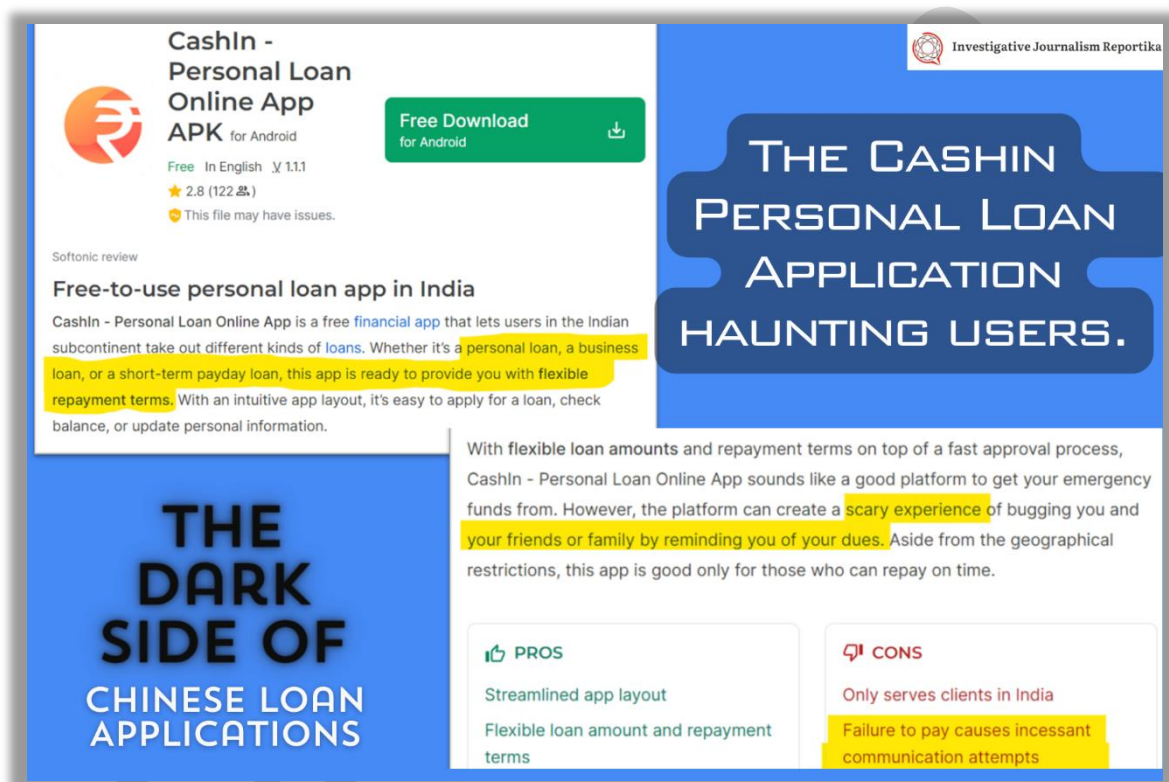


Figure 16 The gut-wrenching reviews of the CashIn Lending Application

Multiple cases have been filed in the Consumer Court of India against the **Mobipocket application** for allegations of blackmail and fraud. Our investigation uncovered several other similar applications engaging in illicit activities, **including Raise Cash, Cash Ray, Infinity Cash, Kredit Mango, CB Loan, Cash Tree, Minute Cash, Cash Light, HDB Loan, SnapItLoan, and Go Cash.** Despite the Indian Government's ban on many of these applications, they persist in some form on the internet through platforms like **Softonic and apkcombo.**



## THE DARK SIDE OF CHINESE LOAN APPLICATIONS

### Fraud by Mobipocket Loan App

Posted on August 21, 2022

Name of Complainant	[REDACTED]
Date of Complaint	August 21, 2022
Name(s) of companies complained against	Mobipocket Loan App
Category of complaint	Cyber Crime
Permanent link of complaint	Right click to copy link

I have applied for a loan on Mobipocket Loan App available on Google Play Store. The app was showing loan of 5600 rupees for 30 days but when loan approved they credited 3920 rupees in my account for 10 days. Means I have applied on 16-08-22 and due date is 25-08-22. So asking for tenure issue [...]

### Mobipocket Loan App

#### Blackmail

Posted on March 7, 2023

Name of Complainant	[REDACTED]
Date of Complaint	March 7, 2023
Name(s) of companies complained against	Mobipocket Loan App
Category of complaint	Banking
Permanent link of complaint	Right click to copy link

I take loan but not paid on time this mobile app increase interest per day 48 rupees now I paid 20000 how to pay i lose my job no money please help me Blackmail was last modified: March 7th, 2023 by Consumer Court

## MOBIPOCKET loan app Fraud Complaints

Investigative Journalism Reportika

Figure 17 Complaints against Mobipocket Loan App in Indian Consumer Courts

## THE DARK SIDE OF CHINESE LOAN APPLICATIONS

### Rupayekey jimmy Anggrean fraud

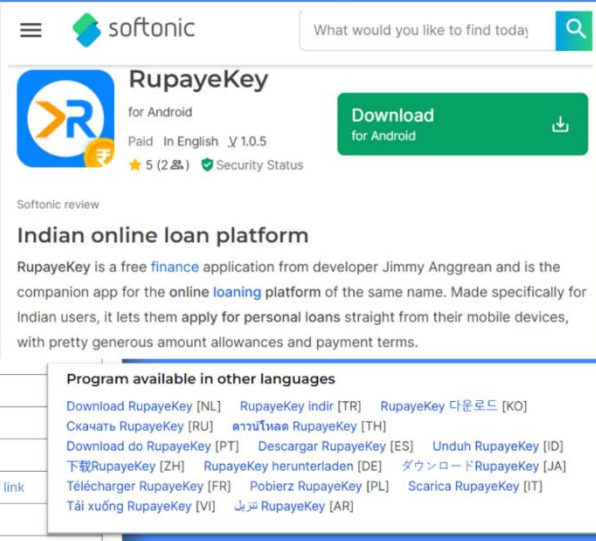
Posted on October 16, 2022

Name of Complainant	[REDACTED]
Date of Complaint	October 16, 2022
Name(s) of companies complained against	rupayekey
Category of complaint	Banking
Permanent link of complaint	Right click to copy link

Share your complaint on social media for wider reach

**Text of Complaint by Zab:**

myslef  
registering a complaint against Rupayekey app. which credited An amount of 2520Rs as a Loan without my permission. they are requesting to close the loan by replaying 4200Rs on 20/10/2022. which i didn't requested from them  
i was hoping a help from the legal side to figure out their scam and giving me the justice



**RupayeKey loan app Fraud Complaints**

Investigative Journalism Reportika

Figure 18 Complaints against Rupaye Key Loan App in Indian Consumer Courts

## IJ-Reportika Survey

In our recent comprehensive survey conducted in India, which reached a significant sample size of **100,000 individuals** (age group **25-40 years**) through a combination of online and offline modes in major cities, including **Delhi, Mumbai, Kolkata, Chennai and Ahmedabad**, the findings underscore the challenges associated with Chinese loan applications.

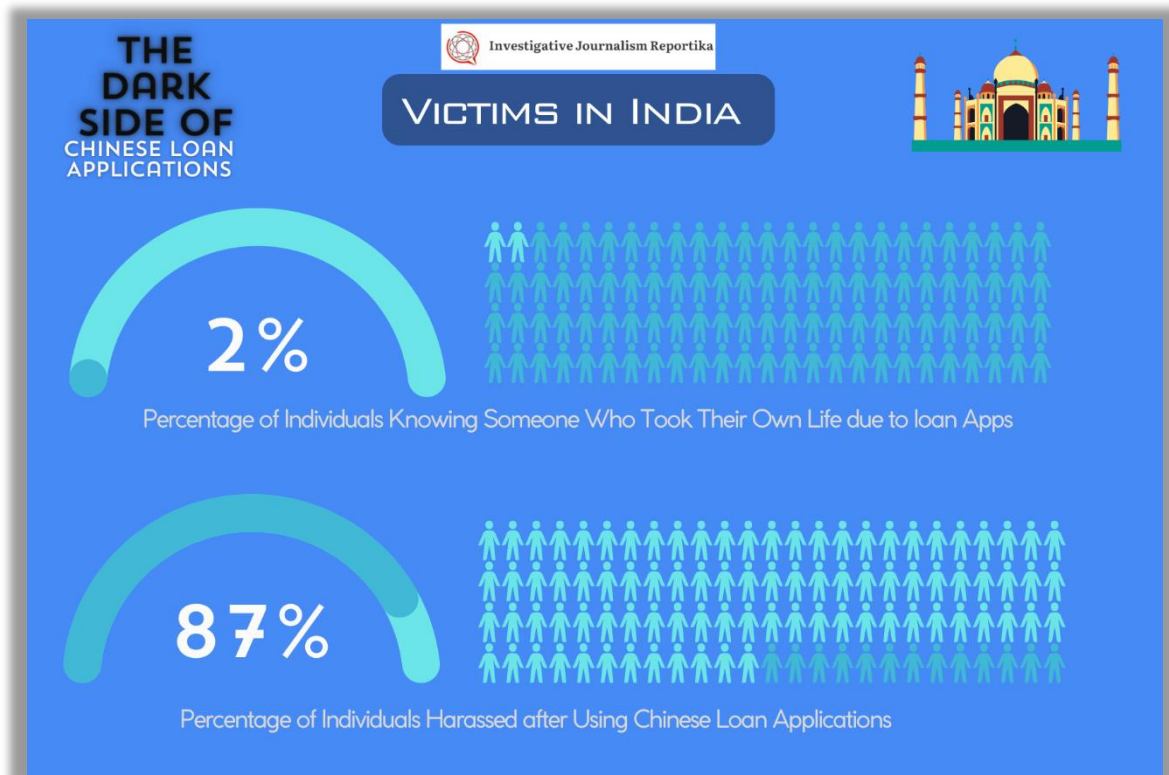


Figure 19 Ij-Reportika Survey Results in India

Within this group, in 2023, **150 individuals** admitted to using Chinese loan applications, revealing distressing outcomes. A substantial **86.67%** (130 out of 150 individuals) reported instances of **harassment** subsequent to their engagement with these platforms. Furthermore, the study brought to light a deeply troubling aspect, with **2%** (3 individuals) of respondents disclosing that they personally knew someone who had **taken their own life**, attributing the tragic event to the pressures associated with these loan applications.

The survey also highlighted that a significant number of those harassed were from the **Lower Middle Class or had faced health emergencies**. Adding to the complexity of the situation, the survey also unveiled the rise of homegrown scam applications in India, mimicking the deceptive practices of Chinese loan applications

## Pakistan

In Pakistan, a surge in rogue lending apps is wreaking havoc on unsuspecting consumers. The **Ij-Reportika** has **unmasked over 93 online lending applications as scams**, engaging in predatory lending practices that involve **blackmail, harassment, and blatant violations of borrowers' data privacy**. Our investigation has revealed the involvement of both domestic and Chinese companies in this digital loan racket, with names like **Flexi Money, Hazir Loan, Credist, Fori Money, Fast Cash, Mr Loan, V Cash, and Mera Rupee** were seemingly dubious applications. A host of these applications are available on the internet with the developer named **LE THUY DUNG** in Pakistan.

The Securities and Exchange Commission of Pakistan has banned over **120 loan applications** in the country to save people from falling into "**debt traps**".

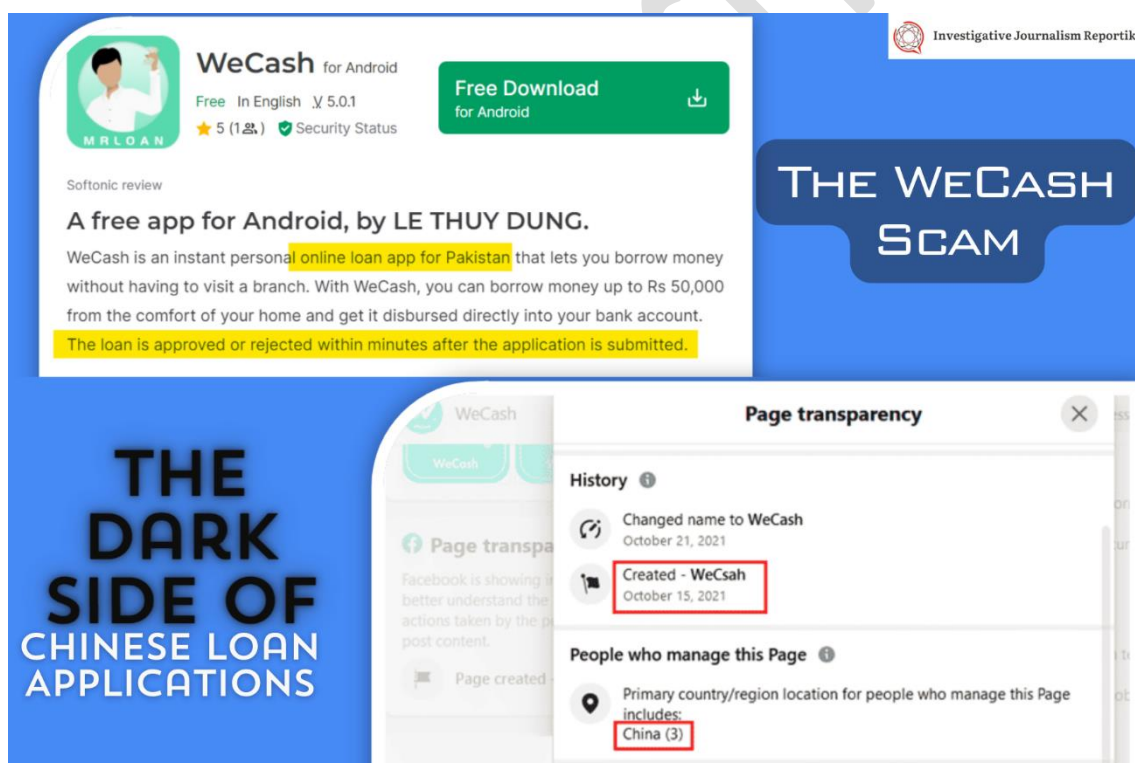


Figure 20 Exposing Chinese Linkage with WeCash Lending App

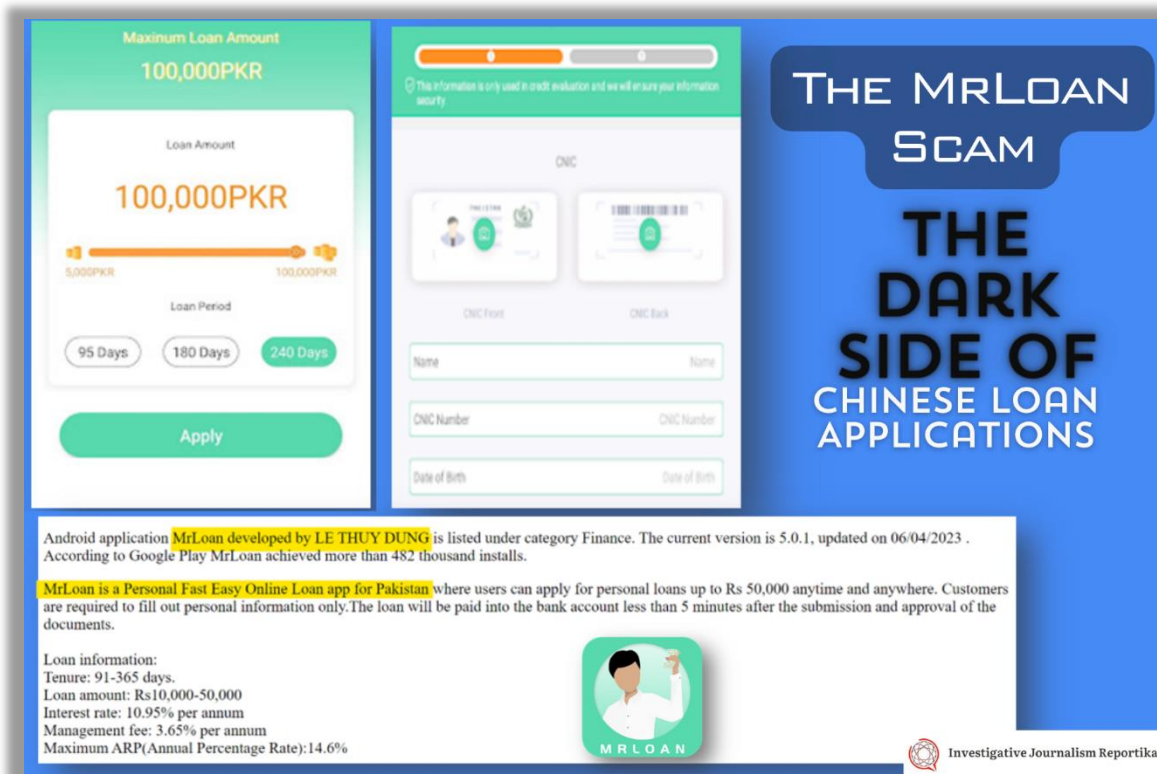


Figure 21 Exposing Chinese Linkage with MrLoan Lending App

Many of these entities, masquerading with fake addresses and unauthorized use of the SECP's name, have connections to **Chinese companies**, echoing patterns observed in **South Asian and Southeast Asian countries like India, Bangladesh and Philippines.**

Against the backdrop of Islamabad's severe macro-economic crisis, marked by a challenging economic environment, a distressed labor market, reduced remittances, surging prices, and the aftermath of natural disasters, household incomes are plummeting, pushing poverty rates to an alarming **37.2%**. Moody's warns that a substantial chunk of revenue dedicated to interest payments is placing a strain on Pakistan's ability to manage its debt while meeting essential social spending needs. **In this increasingly dire economic landscape, fraudulent app-based loan schemes find fertile ground to exploit vulnerable individuals in Pakistan.**

In the grim statistics spanning 2023, the toll of **suicides** in Pakistan reached a **staggering 67** and over Twenty Thousand harassment incidents. The reported incidents we uncovered through Pakistani sources reveal a distressing panorama of individuals driven to desperation by the ruthless exploitation propagated by illicit digital lending apps.





Figure 22 Tragic Tales of Lending Scams from the Pakistani Newspapers

Following is a sample of the suspicious loan applications running in Pakistan.

- 360 Online Qarz
- 567 Speed Loan
- 99 Fast Cash Loan
- Aasan Lab
- Apple Qist Qarz
- Asaan Qarza- credit loans
- Bee Cash
- BG Loan
- CashCredit-Online Loan
- CashPro
- CreditLoan
- CredStar
- Debit Campsite
- DiDi Loans
- Easy Cash Loans
- Easy Loans
- Easy Mobile Loans
- Fair Loans
- Fast Loan
- Fast Manne Loan
- FinMore
- Fori Instant Loans
- Fori Qarz
- Pakkicash
- Pakket Pocket
- Get It Now
- Get Welfare
- HamdardLoan
- Harsha Tube
- Hayar Pocket Easy Fund
- JaidiCredit
- LendHome
- Little Cash
- LoanClub
- MiniLoan
- Money bee
- MoneyBox
- MrLoan
- MY Cash
- MyCash
- Naqad Qarza-ABC
- Plati Loans
- Private Credit
- Galaxy Loan
- OK wallet
- ColeCash
- Focus loan
- Wcash Loan
- LuckMoney
- Pyoor Pack
- Qarza Pocket
- QuickCash
- Rico Box
- Rose Cash
- Sallam Loan
- Superb Loans
- Swift Loans
- Tazza Center
- TiCash
- UrCash
- Whale
- YoCash
- Zenn Park
- ZetaLoan
- Money Club
- Super Magic
- Easy Pocket
- Monii Pro
- Holiday Loan
- Credit Now
- EasyLoan Lite
- Haath Pocket
- Candycash



## IJ-Reportika Survey

In our recent extensive survey conducted in Pakistan, encompassing a sample size of **50,000 individuals (age group 25-40 years)**, we observed noteworthy trends related to the usage of Chinese loan applications. The study covered major cities, including **Karachi, Lahore, Islamabad, and Peshawar**.

Within this demographic, in 2023, as many as **170 individuals** acknowledged using Chinese loan applications, exposing a concerning reality. Out of these users, a substantial **89.41%** (152 individuals) reported instances of **harassment** subsequent to their interaction with these platforms. Furthermore, **2.9%** of respondents (5 individuals) disclosed that they personally knew someone within this demographic who had **tragically taken their own life**, attributing the distressing event to the pressures associated with Chinese loan applications.

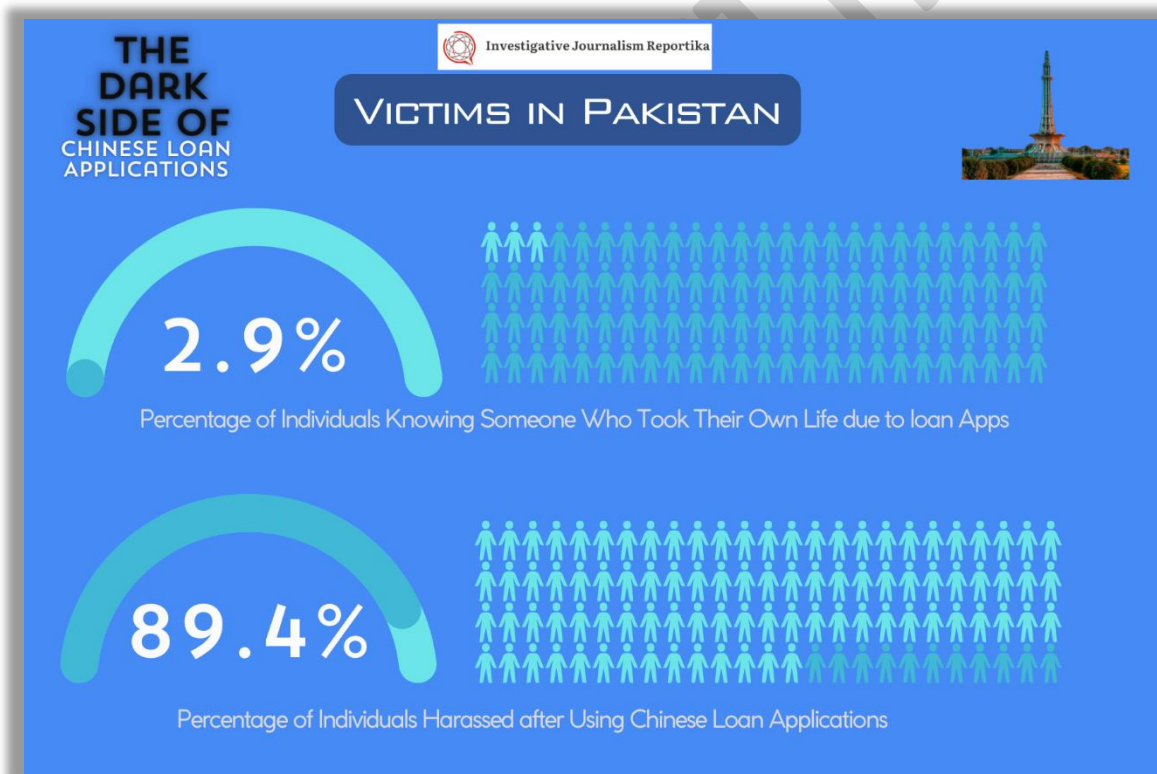


Figure 23 Ij-Reportika Survey Results in Pakistan

Complicating matters further, concerns were raised about the lack of assistance from local police and central authorities, with fears that their pleas were either ignored or overlooked. Disturbingly, it was suggested that suicide cases related to these applications might be significantly underreported due to the sensitive nature of the situation involving Chinese applications, potentially posing diplomatic challenges between the two countries.

## Africa

Chinese loan app scams in African countries, as extensively discussed in this report, mirror patterns seen globally. **Unregulated lenders offer small, high-interest loans, pressuring borrowers to provide personal information as collateral.**

Some of the loan apps that have been involved in these scams are:

- **KashBean:** The loan packages offer amounts from 1,500 KSh to 80,000 KSh with interest rates ranging from 0% to 36% per annum. Despite emphasizing transparency, the app lacks clarity on potential hidden costs. Additionally, borrowing 20,000 KSh for 91 days incurs a total payment of 7,266 KSh. It has a very poor ratings due to its poor customer service.

The image is a composite graphic with a blue background. At the top left, it says "THE DARK SIDE OF CHINESE LOAN APPLICATIONS". At the top center, a dark blue banner reads "KASHBEAN SCAM IN KENYA". On the left, there's a screenshot of the Kashbean app interface showing a "Maximum loan amount(KSh)" of 80,000 and a "Borrow now" button. Below that is a screenshot of the Facebook page for "Kashbean", which is an "Internet company" with 2.3K likes and 2.7K followers. The address "Applewood Building, Nairobi City, Kenya, Nairobi, Kenya" is highlighted in yellow. On the right, a "Page transparency" window is open, showing "Page information for Kashbean" and "History" (Created - November 3, 2022). Under "People who manage this Page", it lists "Primary country/region location for people who manage this Page includes: China (2), Kenya (2), Not available (1)". A red arrow points from the "China (2)" entry to the text "PAGE ADMINS: CHINA" below. At the bottom left, it says "ADDRESS : KENYA" with a red arrow pointing to the address in the Facebook page screenshot. At the bottom right, there is a logo for "Investigative Journalism Reportika".

Figure 24 Exposing Chinese Linkage with KashBean Lending App



Figure 25 Users Calling out the Scam of KashBean Lending App

- Okash:** An app that offers loans ranging from 2,500 to 50,000 Kenyan KSh (about \$23 to \$460) with a repayment period of 14 to 91 days. The app charges an interest rate of 24% and a service fee of 14%. The app has been accused of sending abusive and vulgar messages and calls to borrowers and their contacts, as well as accessing their photos and social media accounts.

## THE DARK SIDE OF CHINESE LOAN APPLICATIONS

## OKASH SCAM IN KENYA

IT HAS LENDING AS WELL AS GAMBLING GAME OPERATIONS IN KENYA AND OTHER AFRICAN COUNTRIES AS WELL

**OKash**  
@OKash\_Kenya

OKash is a mobile lending app that seeks to empower the average Kenyan through availing short term loans

Nairobi, Kenya | o-kash.com | Joined January 2019

ADDRESS : KENYA

Page information for OKash APP Kenya

**History**

- Changed name to OKash APP Kenya (January 4, 2022)
- Changed name to OKash APP Kenya (January 4, 2022)
- Created - OKash APP (December 10, 2020)

**People who manage this Page**

Primary country/region location for people who manage this Page includes:

- China (6)
- Taiwan (2)
- Not available (2)

PAGE ADMINS: CHINA AND TAIWAN

Figure 26 Exposing Chinese Linkage with OKash Lending App

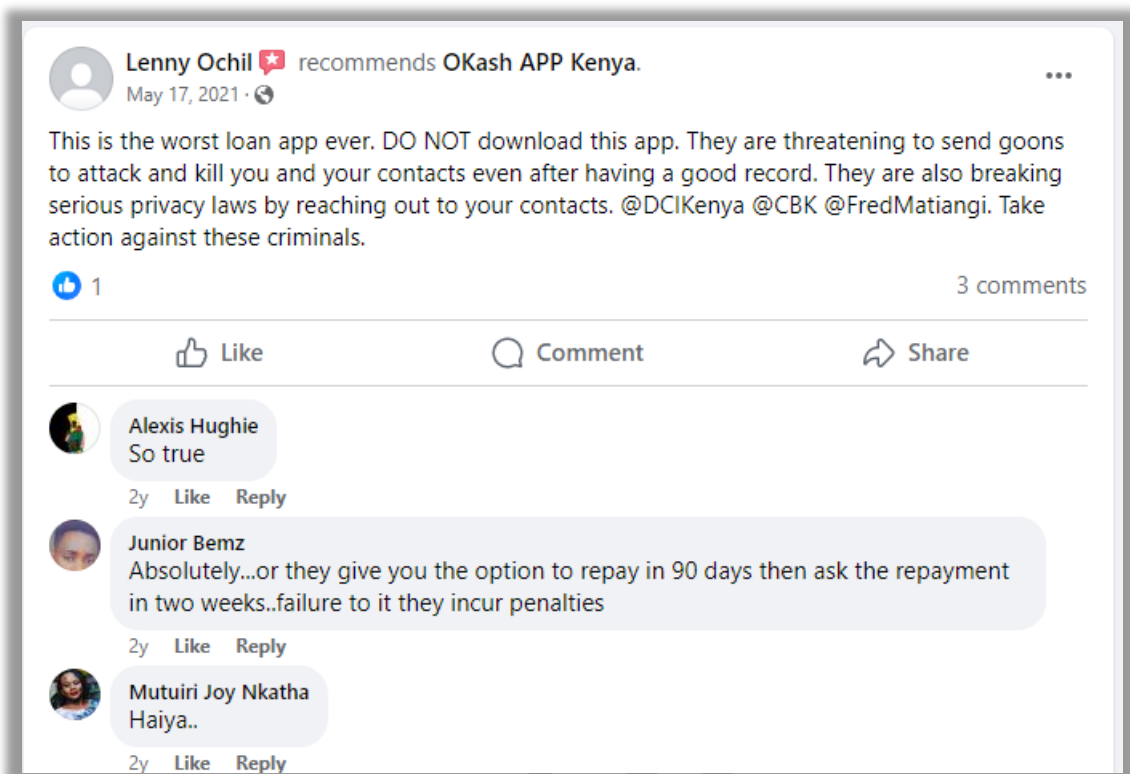




Figure 27 Users Calling out the Scam of OKash Lending App

- **Opesa:** An app that offers loans ranging from 2,000 to 30,000 Kenyan shillings (about \$18 to \$276) with a repayment period of 14 to 91 days. The app charges an interest rate of 16% and a service fee of 9%. The app has been accused of sending threatening and humiliating messages and calls to borrowers and their contacts, as well as accessing their photos and social media accounts.
- **Palmcredit:** An app that offers loans ranging from 2,000 to 100,000 Nigerian naira (about \$5 to \$245) with a repayment period of 91 to 180 days. The app charges an interest rate of 14% and a service fee of 12%. The app has been accused of sending threatening and humiliating messages and calls to borrowers and their contacts, as well as accessing their photos and social media accounts.

**THE DARK SIDE OF CHINESE LOAN APPLICATIONS**

**PALMCREDIT SCAM IN NIGERIA**


**₦300,000 in 5 minutes**

Now available on  

**Palmcredit**  
391K likes • 424K followers

**Page transparency**

Page information for Palmcredit

 Palmcredit  
Financial service

History

Created - Palmcredit  
May 7, 2018

People who manage this Page

Primary country/region location for people who manage this Page includes:  
Nigeria (9)  
China (6)  
Japan (1)

**PAGE ADMINS: CHINA**

**HUGE FOLLOWING ON THE PAGE**





 Investigative Journalism Reportika

Figure 28 Exposing Chinese Linkage with PalmCredit Lending App

 **Macdonald Peters**  
August 4 · 🌐

Fraudulent loan company #palmcredit  
[Palmcredit](#)  
Palmcredit Response

Palmcredit Hello to whom it may concern kindly take back the money you sent to my account below.

Account:   
Bank Name: 

For your information I will not take that money because I did not request for any loan from your useless Palmcredit.

I have heard how you guys are scamming people by punching in money into their account's stupid people.

Why will you send my kid brother who is below 18years  
N120,000 are you okay.

The best you take your money or I will make up a document with this and get a lawsuit.

Fock you all!


 1 4 comments

Figure 29 Users Calling out the Scam of PalmCredit Lending App



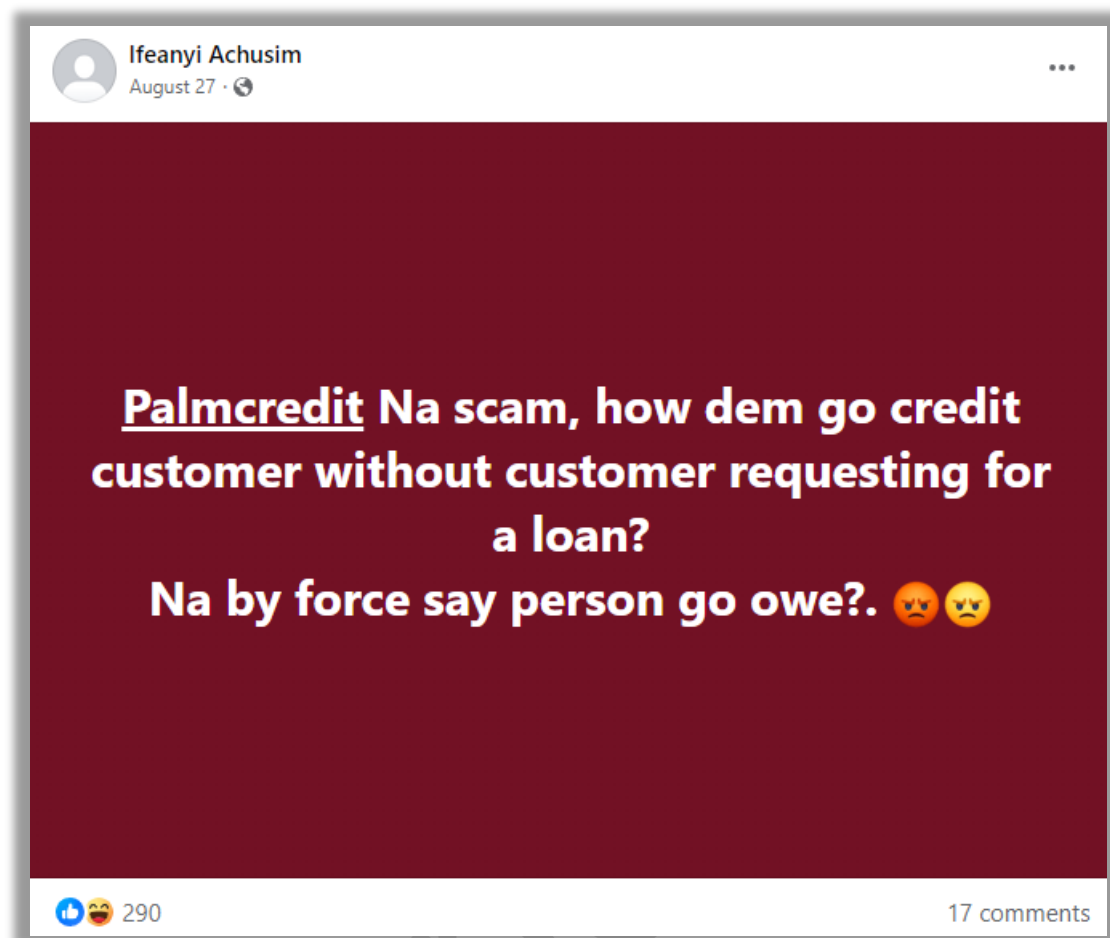


Figure 30 Users Calling out the Scam of PalmCredit Lending App

- **Branch:** An app that offers loans ranging from 1,000 to 200,000 Nigerian naira (about \$2 to \$490) with a repayment period of 4 to 64 weeks. The app charges an interest rate of 15% and a service fee of 10%. The app has been accused of sending abusive and vulgar messages and calls to borrowers and their contacts, as well as accessing their photos and social media accounts.
- **Carbon:** An app that offers loans ranging from 1,500 to 1,000,000 Nigerian naira (about \$4 to \$2,450) with a repayment period of 4 to 64 weeks. The app charges an interest rate of 16% and a service fee of 8%. The app has been accused of sending threatening and humiliating messages and calls to borrowers and their contacts, as well as accessing their photos and social media accounts.

These apps are among the many online lending services that have been operating in Africa without proper regulation and oversight. The African governments and regulators have been taking measures to stop these illegal lending apps and their operators, as well as to protect the rights and interests of the borrowers.

For instance, in response to an escalating issue involving **unlicensed Chinese loan applications**, the Bank of Ghana has issued a cautionary notice, highlighting a **breach of the Banks and Specialised Deposit-Taking Institutions Act, 2016 (Act 930)**. Collaborating with relevant state agencies, the central bank is steadfast in taking action to uphold the integrity of financial service delivery.

The public is strongly advised against engaging with unlicensed loan providers, most of which have **links with Chinese companies**. The Bank of Ghana underscores the potential infringement of customer data and privacy laws, emphasizing the adverse impact on consumer protection and financial system integrity. Users are encouraged to opt for **digital credit products** approved by the Bank of Ghana and delivered by **licensed institutions**. Below is a list of unauthorized loan applications operating in the market:

- Flash Cash
- GhLending
- MoLoan
- Rapidcedi
- 100 Cedi
- Cedi Help
- Mascedi Consult
- Cediboom
- CashLoanPro
- Aircash
- Akwaaba Payment
- FourCredy
- Ghanalending
- AcornCredit
- Gana Loan
- Mach Loans Ghana
- Mbose
- Sika Bus
- Sikakasa
- Chasteloan
- Joy Cash
- Cocoaloan
- Popcash
- Loan hub
- Creditmall
- cedipros
- Momcash
- GETwallet
- Keeploan
- CashCocoa
- Bitcash
- Ukash
- Ultra Loan Fund
- Cedi Ghana
- Loan App
- Mika Cash Loan App
- New Loan Ghana
- Zip Loan
- Credit Ghana App
- Bloomcash
- Home Credit
- AkwaabaCash
- Cash Way
- Momo cash loans
- Prime Loans
- Easy Access Loans
- Cashpal Online Loan
- Happy Loan
- Money Loan App
- Plus Loan
- Mega Credit
- Boeing Cash
- Lemon Wallet
- Koko Cash
- Cola Cash/Cash Cola
- Rapid money
- Hello Cedi/Sunny Cash
- Goldminer
- Enjoy Credit
- Cash Star
- Loan Galaxy
- MOCO
- Funcash
- Cedi Wallet
- Pro Kash
- Cedi Fie
- HelaCash
- Daily Cash
- FiCash
- Sikadua
- PK Loans
- Quick Cash
- True Cedi
- Robin Personal Loan
- Kudi Credit
- 1 Rapid cedi
- Cedistory
- Steadycash
- Soft kash
- Easy Kash
- DatesCash
- Boseapa
- YooCash
- Fufucredit
- TopCredit
- DeriveCash
- Eagle Cash
- Cash wave
- cud loan
- smatloan
- LoanPapa
- CoolCash
- MoLoan
- Rapid Cedi
- cedifie



Figure 31 Exposing Chinese Linkage with Akwaaba Lending App

The Chinese loan app scams in Africa and other countries expose the risks and challenges of the online lending industry, especially for the low-income and vulnerable groups who lack access to formal and regulated financial services. They also call for more cooperation and coordination among the governments, regulators, and law enforcement agencies of different countries to prevent and combat these cross-border cybercrimes.

#### IJ-Reportika Survey

In our extensive survey conducted across **Nigeria, Kenya, and Ghana**—specifically in cities such as **Lagos and Abuja** (Nigeria), **Nairobi and Mombasa** (Kenya), and **Accra and Kumasi** (Ghana)—we gathered data from a sample size of **200,000 individuals (age group 25 to 40)**, shedding light on the pervasive use of Chinese loan applications in the African context.

Within this demographic, a whopping **3,650 individuals** admitted to using Chinese loan applications, a significant revelation considering the associated challenges. Among these users, a substantial **93.4%** (3,412 individuals) reported instances of **harassment** following their interaction with these platforms. Furthermore, **1.56%** of respondents (57 individuals) disclosed that they personally knew someone within this demographic who had **tragically taken their own life**, attributing the distressing event to the pressures associated with Chinese loan applications.

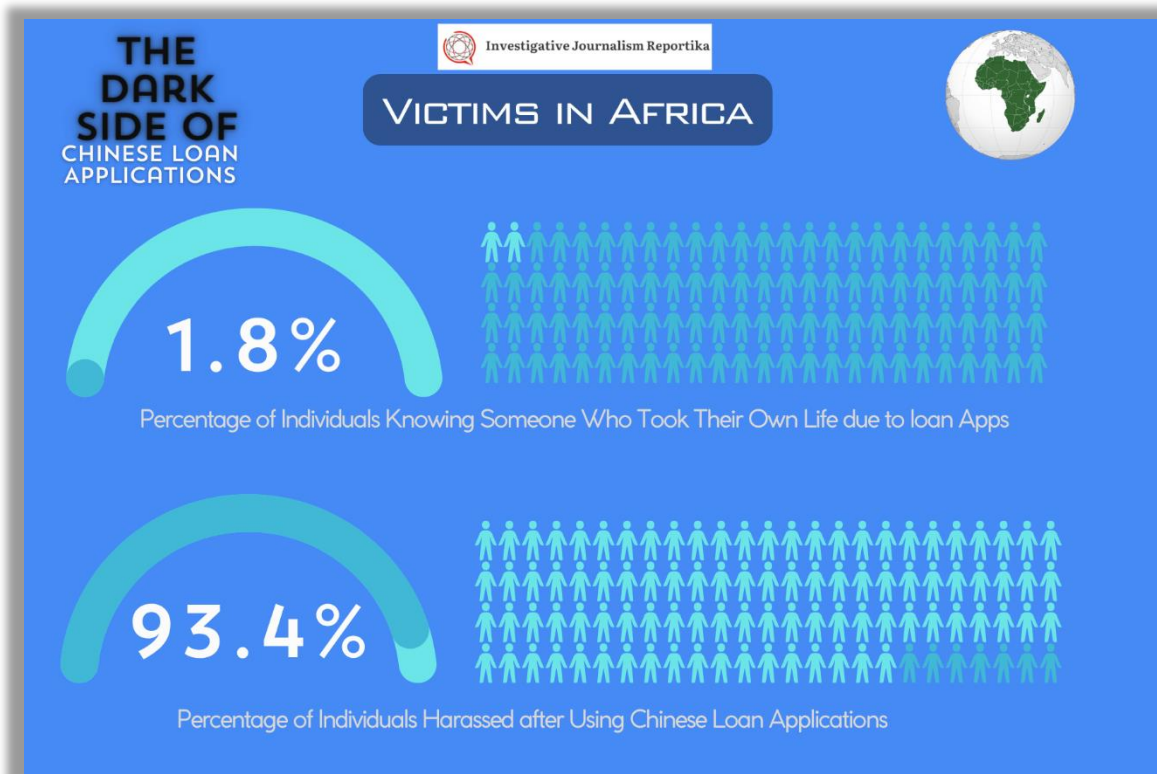


Figure 32 Ij-Reportika Survey Results in Africa

Compounding the issue, regulatory steps taken by **Nigeria and Kenya** were deemed **inadequate**, and in Ghana, despite government officials pointing out the shortcomings, backdoors like **TikTok and Facebook groups** remain available to dupe people with these applications. Most individuals in the sample belonged to the **poor and lower-middle-class segments**, seeking funds to start small businesses and sustain their families.

A notable contrast emerges in **the Chinese agents' behavior, openly displaying their identities in African countries, unlike in other nations where they remain hidden**. Governments in Nigeria, Kenya, and Ghana, according to our investigation with government officials, seem to **downplay suicide and harassment cases** to preserve diplomatic relations with **China**, due to their considerable **debt burden from Belt and Road Initiative (BRI)** projects.

Our prior reports extensively investigated the status of **stalled Belt and Road Initiative (BRI) projects** and drew attention to the presence of **Chinese fishing ships in the Exclusive Economic Zones (EEZ) of several African countries**. These findings suggested a prevailing trend of governments of most African countries overlooking critical issues to preserve diplomatic relations. Our investigation, involving discussions with government officials, confirmed this trend and indicated that such actions is influenced by the significant **debt burden resulting from BRI projects**.

## **Protective Measures Against Chinese Loan App Scams**

To safeguard against Chinese loan app scams, individuals are advised to take the following preventive actions:

### **1. Verify Lender Legitimacy:**

- Do not use unlicensed and untrustworthy online lending services.
- Always check the legal status and reputation of lenders before applying for loans.

### **2. Protect Personal Information:**

- Avoid giving access to personal information, including ID cards, bank accounts, phone numbers, and social media accounts, to any online lenders.
- This information can be exploited for scams and harassment targeting you and your contacts.

### **3. Exercise Caution with Apps:**

- Do not download any apps recommended or required by online lenders.
- Such apps may increase your debts or compromise your data security.

### **4. Report Suspicious Activities:**

- Report any suspicious or fraudulent activities to the authorities.
- If scammed or harassed by online lenders, promptly contact the police and relevant agencies to file a complaint and seek assistance.

These individual-level precautions, when coupled with international collaboration and government efforts, contribute to creating a safer online lending environment for everyone.

## **Conclusion**

The Chinese loan app scams are a global phenomenon that affects millions of people who need quick cash. These scams involve unlicensed and unregulated online lenders that offer small loans with high interest rates and short repayment periods. The borrowers are asked to provide personal information, such as ID cards, bank accounts, phone numbers, and social media accounts, as collateral for the loans. If they fail to repay on time, the lenders harass and blackmail them and their contacts with abusive messages, calls, and photos. Some of the victims are also forced to download more apps that increase their debts or steal their data.



These scams have been reported in many countries, such as India, Philippines, Vietnam, Nepal, Bangladesh, Myanmar, Kenya, Nigeria, Ghana, and South Africa. The governments and regulators of these countries have been taking measures to stop these illegal lending apps and their operators, as well as to protect the rights and interests of the borrowers. However, these scams are still prevalent and pose a serious threat to the financial security and well-being of the low-income and vulnerable groups who lack access to formal and regulated financial services.

The Chinese loan app scams are a serious problem that needs to be addressed by the governments, regulators, and law enforcement agencies of different countries. They also need to cooperate and coordinate with each other to prevent and combat these cross-border cyber crimes. Moreover, the public needs to be educated and informed about the risks and challenges of the online lending industry and the ways to protect themselves from these scams. By taking these actions, we can hope to create a safer and fairer online lending environment for everyone.

## References

- <https://consumercomplaintscourt.com/rupayekey-jimmy-anggrean-fraud/>
- <https://sundayguardianlive.com/news/chinese-loan-apps-pose-threat-india>
- <https://apkcombo.com/rupayekey/com.app.rupayekey/>
- [In India, some of the apps that have been involved in these scams are CashBean, Okash, Opesa, Zenka, Palmcredit, Branch, and Carbon.](#)
- [In Kenya, some of the apps that have been involved in these scams are CashBean, Okash, Opesa, Zenka, MTN Qwikloan, and Lime.](#)
- [In Myanmar, some of the apps that have been involved in these scams are RupeeGo, Rupee Here, LoanU, QuickRupee, Punch Money, Grand Loan, DreamLoan, CashMO, Rupee MO, CreditLoan, Lendkar, RockOn, HopeLoan, Lend Now, and Cashfull.](#)
- [In February 2022, the Philippine National Police - Anti-Cybercrime Group \(PNP-ACG\) arrested 46 suspects, including a Chinese national, who were allegedly behind several lending apps that scammed thousands of Filipinos](#)
- [The suspects were charged with violation of the Cybercrime Prevention Act of 2012](#)
- [The SEC warned the public to be cautious and to take measures before engaging in online transactions to avoid being victims of online fraud](#)
- [The Securities and Exchange Commission \(SEC\) also banned 19 lending apps that were operating without a certificate of authority or license in the Philippines](#)
- [In November 2023, the Detective Branch \(DB\) of Police arrested 15 people including a Chinese national for operating loan scams through social media](#)
- [The suspects were charged with violating the laws on credit institutions, cyber security, and telecommunications](#)
- <https://techwireasia.com/12/2023/how-do-new-malicious-fake-loan-apps-work/>
- [The African governments and regulators have been taking measures to stop these illegal lending apps and their operators, as well as to protect the rights and interests of the borrowers](#)