



Widespread UPI Scamming Group Actively Defrauds Indian Public

Report Summary

In the last few years, India has seen a surge in the usage of digital wallets and online payments systems such as BHIM, Google Pay, Paytm, and Phonepe. So much so that, Unified Payments Interface (UPI) recorded a whopping 10.8 billion transactions in 2019, becoming the most preferred payment method, well ahead of IMPS, debit, and credit cards. Touted as the fastest product to reach 1 billion transactions a month, people have made a habit of using UPI for daily payments. However, this has encouraged scammers to defraud the Indian public by exploiting UPI users.

Recently, CloudSEK's digital risk management tool [XVigil](#) identified a mobile number: +91 9004676782 that is linked to various UPI related scams. We found that scammers often use this number in conjunction with other mobile numbers, many of which we have identified. Based on the mobile numbers, our research team uncovered a large group that is operating a gamut of UPI related scams. From the mobile numbers, we estimate that the group has at least 3 branches, 1 each, in West Bengal, Uttar Pradesh, and Maharashtra.

Our research indicates that the scamming group is performing various scams apart from UPI fraud alone. Among them two interesting ones are hosting fake e-commerce websites and fake justdial pages for legitimate businesses. They are targeting various business sectors, including ecommerce, banking, and aviation. Despite complaints on the internet, news coverage of their scams, and First Information Reports (FIRs) lodged by victims, the group continues to operate successfully, with impunity.

In this article, we detail our research findings on the scamming group's operations and tactics, along with attributing them to individuals likely running the scams.

Why is +91 9004676782 so infamous?

Facebook page of 9004676782



9004676782

Home

Posts

Reviews

Photos

About

Community

Create a Page

Victims, and potential victims, have reported several mobile numbers, from which they have received sham calls. However, the mobile number most associated with scams involving AnyDesk, SMS frauds, and fake UPI transactions is: +91 9004676782. The infamous number even has a [Facebook page](#).

Since the number is widely used, we found several complaints on online platforms. The victims' grievances show that, even when they don't receive fraud calls from this number, they are asked to send One Time Passwords (OTPs), Personally Identifiable Information (PII), Know Your Customer (KYC) details, and UPI Account activation numbers (UPIACT) to it.

Mobile Location : Mumbai, Mumbai metro telecom
Truecaller Name : Axis Axisbank (Bank)
Reported as spam : 8,897 times
Operator : Airtel

This number was identified as the key suspect linked to all the scams. So, we retrieved all other numbers affiliated with it, which in turn assisted in determining the scamming group.

The group is actively scamming people everyday

The number has been mentioned in a news article about a scam, carried in the Hindi newspaper Dainik Bhaskar's UP edition, on 23 June 2019.

[Nagpur daily](#) also covered a scam on 24 July 2019, about a man in Jaitala who was defrauded by a fake MakeMyTrip agent. And unsurprisingly, the fake agent had asked him to forward a link to **+91 9004676782**. Soon after, he received withdrawal alerts from SBI and HDFC.

Apart from mainstream news coverage of the mobile number, there are several reports on social media, complaint forums, and other online platforms. Victims have even lodged FIRs, despite which the scamming group is active, and continues to use the same number to scam people across business sectors.

DainikBhaskar article

लगेज की बुकिंग के नाम पर उड़ाए 28500

लखनऊ। आस्ट्रेलिया के न्यू साउथ वेल्स निवासी राहुल टंडन के लगेज की बुकिंग के नाम पर उसके रिश्तेदार के खाते से 28500 रुपये उड़ा दिए। राहुल की तरफ से सिंगारनगर आलमबाग निवासी रिश्तेदार देवेन्द्र कुमार धवन ने एफआईआर दर्ज करा दी है। साइबर सेल की मदद से पुलिस जांच कर रही है। इंस्पेक्टर योगेंद्र प्रसाद ने बताया कि देवेन्द्र के बेटे की 18 मई को शादी थी जिसमें राहुल टंडन भी शामिल हुए थे। वापसी के वक्त राहुल के पास काफी सामान हो गया था। उन्होंने लगेज के किराए के बारे में जानकारी लेने के लिए एयर इंडिया के कस्टमर केयर नंबर 07608968314 नंबर पर संपर्क किया। उक्त नंबर राहुल ने गूगल से लिया था। देवेन्द्र ने बताया कि ठगों ने राहुल को दूसरा मोबाइल नंबर **9004676782** देते हुए उस पर संपर्क करने को कहा।

Fake Customer Care

Aziz Alam Qureshi @AzizQureshi
Replying to @RailwaySeva
Have you appoint any executive for dealing the tweets reply? I recd a call from +919875656747 saying I am Frm IRCTC to resolve ur complaint He will refund instantly they send me a sms of 1 Rs by UPI saying to frwd this sms to 9004676782. Reply me please

Modi's supporter @KaranUp05224051
@zomatocare hello sir 8389097901 is faud no. In name of zomato my friend sent me this no for refund when I call him then they ask for upi pin and sent me another no. 9004676782 for sent my personal details please take some strict action against all frauders like him

Regarding money stolen complain from ATM.
Dear sir,
on 01/02/19 an amount of 62,900 is hack / stolen from my A/C no. 913010006819813 which fact regarding the money stolen details are.
1. I had done shopping from the club factory before 3 months and the price was deducted from Axis account 913010006819813 of Rs. 1653.
2. Goods were not received as it was gone back, undelivered.
3. I waiting for refunding my money but not refunded till 01/02/19.
4. At about 1600hrs. of 01/02/19 I got some nos. from the club factory's website and I made a call in the no. +917326072126.
5. He said money will refunded immediately but you have to send message in the no. 9004676782 immediately within 10 second. He enquired my card's last 4 digit no. 1399 with expiry date 04/22.
6. With this message I sms OTP 840990 to 9004676782 and as soon as I shared OTP Rs. 62,900 was deducted from my account immediately.
and I give all the details to UPI officer within half hour. the service request no. given by UPI officer is 48562126. Next day all the details with police FIR submitted to near bank branch and also mail to Paytm.
after all these, I receive message from Axis three times as my money is credited (screen shots enclosed) out of 62,900 an amount of 42,900 is temporarily credited but not received till date.
Regarding this kindly help me I shall be ever remain thankful to you.

Sagar Harwani @HarwaniSagar
@goibibo Got a call from this number +919875656747 saying that he is from Goibibo and asking me to forward the message on 9004676782. Do you follow this practice or its a spam ?

vinay tinaikar @VinayTinaikar
@Cleartrip got call from +916289816297, 9004676782 asking for bank details for refund, is it valid?
10:26 am · 21 Aug 2019 · Twitter for Android

Cleartrip @Cleartrip · 21 Aug 2019
Replying to @VinayTinaikar
Dear Vinay, do not give any bank details to anyone. We have already processed your refund in your original mode of payment. We do not require

#paytm #paytmcare siSomebody call me from this number 9382611309. He said to me forward message to this number 9004676782 I would like to know about it. Was it authorised Paytm call.

NAMAN KUMAR @nmanankumar
Seriously!!!
I got a call from a fake executive just after I tweeted to you
You are reading
I got call from this number 6281332039
He told me to fwd the sent msg by him on these numbers which has a link to directly cut the amount in your bank account
7304499902
9004676782

IRCTC West Zone @irctcwestzone · 8 Aug 2019
Replying to @RailwaySeva and @nmanankumar
Matter is being taken for necessary action.

TanujaSood posted this 11 August 2019

06204563994 this is a mobile number of the person who is making people fool by writing on Twitter and many online platforms that this number is Myntra customer care number. This person has lotted Rs.3000 from my bank account.

I had to return a product which I bought from Myntra but I wasn't able to put return request on their website so I decided to call on their customer care number which I googled.

But after calling twice on that number my call didn't get through so I searched more n got this number from a Twitter link and it was described as myntras customer care no.

I called on this no., a guy picked up the call, I asked him that is this Myntra no? He said yes and then I told him about the problem I was facing regarding the return of the product.

To which he asked for the barcode of the product and the order I'd and asked in which bank do I need the refund.

I told the name of my bank and after which he said he will send me a message mobile no is (8638247958) and I need to send it to other number i.e. 9004676782 and then he will transfer the amount in my account.

venugopal Kolla @venugopal_kolla
Hello sir @hydcitypolice @cyberabadpolice @cyber i got a cal from 9102604336 as @PhonePe CC and asked me complete my KYC so he asked to send below SMS got from #8076972063 to this #9004676782 to activate. It's fraud call as today #RepublicDay
Kindly take action on this.

harsh Modi ek bar fir se @mauryas
@CPDelhi Respected Sir,
With due respect, I would like to inform you, that I got a call from this no. - 9330142953. And the speaker told me that he is speaking from Paytm.

He said that whatever your amount had been deducted and asked me to forward SMS on 9004676782

Santosh Kumar Singh @sksingh1964
But to get so he says I need to follow few steps like -He sends me a message and asks me to forward it to another number i.e. 9330249563 so that the payment can be done by Google Pay.
@makemytrip @PMO @RBI @ZeeNews @bokaropolice
10:14 pm · 24 Jul 2019 · Twitter Web Client

Santosh Kumar Singh @sksingh1964 · 24 Jul 2019
Replying to @sksingh1964
Similarly, this activity was repeated on his personal on different number 9004676782. 9245234567.
@makemytrip @PMO @RBI @ZeeNews @bokaropolice

Fake Mobile Recharge

Rajesh D. Hajare RDH @RDHSir
Mukesh who pretends to be @Paytmcare representative sounded angry but he recharged my @BSNL_MH No. 7588***01 with Rs 10 Top Up & my main a/c credited with Rs 7.475. So I tried to believe him. Then he sent Similar SMS prefixed by ACTIVATE & asked me to FORWARD to 9004676782

Fake UPI Registration

MY MONEY HAS FRAUDED BY THIS UPI

Complain Detail:- Today morning I have received a call from the UPI registration complaints. They told that your account UPI needs to be activated. The problem they told you to need to activate it using the card number and expiry. Details provided by me Mobile number: debit card: Last 4 digit number Expiry date: Caller info : Mobile number : 6294199807 UPI number : 8612684502 @kkbk0008057 Upi activation link received from : +916204866451 Upi link sent to 9004676782 Amount taken: Icc Bank : 6120SBI bank : 1000 Also, they have recharge for : 6204866451 I have received the SMS from ICICI bank for UPI adding purpose. I shared that OTP. After 2 min my amount has been started reducing. They used the Axis bHim app and get the SBI Upi information. I have called Icc bank and blocked the access. Kindly help me get my amount back. I have attached

Fake Mobile Porting

Shreya Narang @narangshreyaa · 26 Jan
@airtelindia @Airtel_Presence My friend wanted to port her number to Airtel, and got this contact from google- 06200106134 - the guy asked us to put our UPI pin in a google doc. When we said no, he persisted that this is the correct way. @DCP_CCC_Delhi

Bharti Airtel India @Airtel_Presence · 26 Jan
Hi Shreya! Thanks for reaching out to us! Please do not respond to any such suspicious calls from unknown numbers asking for personal details. As we never ask customer to share their personal info at any forum. In future, always remember (cont) srkl.in/1/60138LEroD

Shreya Narang @narangshreyaa · 26 Jan
That person gave us this number 9004676782 to send a msg on. Here's that msg
"ACTIVATE b9a14f2312773a1f335b6b4a3e2c750e557f1d72"
@HDFCBank_Cares @DCP_CCC_Delhi
He said his name is Rakesh Mishra and he sits out of Gurgaon

How is the scamming group able to defraud so many people?

Step 1: Identifying the right victims:

- The group posts fake customer care numbers on social media, blogs, and fake websites. They even create fake Justdial pages for legitimate companies. So, when a customer searches online for a company's contact details, these fake numbers show up in the top results. Leading the customer to believe they are contacting the official support line of the company.
- The group actively monitors complaint forums and social media for posts about failed transactions, accidental deductions, refunds, returns, and even feedback on e-commerce vendors. Such posts often contain the customer's sensitive information, including account numbers, order ID, mobile number, and email address.
- Sometimes victims directly receive calls from the scammers. This shows that the group uses data obtained from Open Source Intelligence (OSINT) sources.

As seen below, soon after the victim posted their complaint, along with their ticket information, they received a call from the scammers.

Customer complaint	Customer's interaction with the threat group
<p>Ritika Dube @DubeRitika · Feb 28 @VRLTravels @redBus_in</p> <p>Bus No. is MH09EM4152 Ticket No. TP3V51325104</p> <p>Bus has no live tracking, no light at seat L29, no emergency contact in bus, no response from bus operator.. I mean charging 1260 and no help at all is pathetic..</p> <div data-bbox="224 1381 678 1581" style="border: 1px solid black; padding: 5px;"> <p>Seat No L29 - Vishal Waydande</p> <p>Ticket No TP3V51325104</p> <p>Fare ₹1260.0</p> </div> <p>Bus information and tracking details will be shared on the following number on the day of journey</p> <p>redBus @redBus_in · Feb 28 That's something we didn't wish for, we'll check and get back with an update.</p>	<p>Ritika Dube @DubeRitika</p> <p>Replying to @redBus_in</p> <p>Reporting a fraud activity initiated .. Red bus called and offered refund for the incident and asked to forward msg and fill the below form that is asking for upi pin</p> <p>Call received from 8389986085 Asked to forward messages to 8546995577 and 9004676782</p> <div data-bbox="743 1602 1425 1749" style="border: 1px solid black; padding: 5px;"> <p>redBus Refund Money</p> <p>Description docs.google.com</p> </div>

Step 2: Persuading the victim

When the scammers call the victim or the victim calls the fake number that belongs to the scammers, they need to address the victim's complaint in a believable manner.

- Since customer complaints involve money refunds, the scammer promises refunds via UPI.
- Sometimes the scammers offer extra reward money.
- They even pose as UPI agents who inform the victim that their UPI account needs to be activated again.
- The scammers also use a range of social engineering tactics to appear legitimate based on the target and the service. The scammers use their verbal skills to lure the victims.

Step 3: Collecting sensitive information

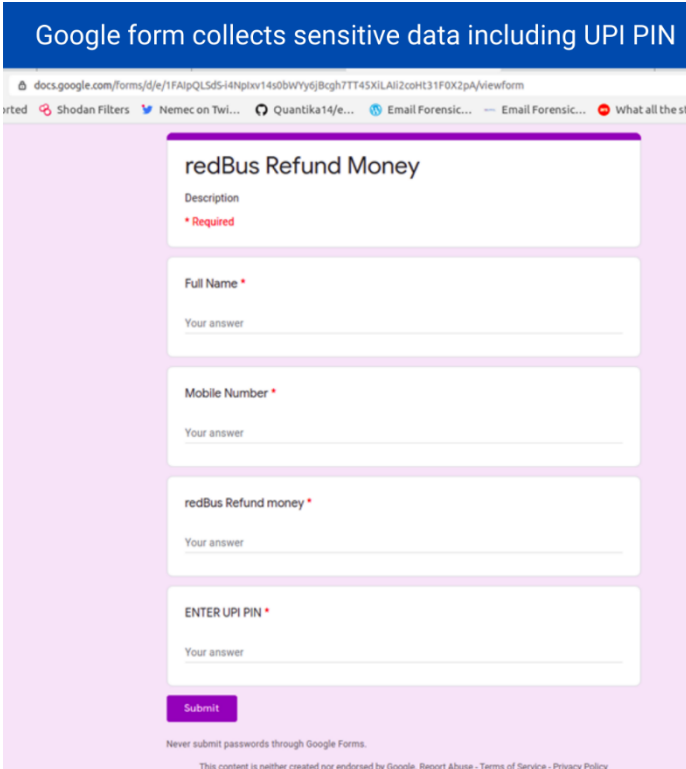
Once the victim has been convinced, the scammer attempts to collect sensitive information such as full name, OTP, debit card or credit card specifics, bank account details, UPI PIN, etc., required to create a UPI account on behalf of the victim.

This information is primarily collected in 3 ways:

- During the phone conversation, the victim gives the scammer their details.
- An official looking [google form](#) that collects sensitive data such as name, mobile number, and UPI PIN. By sending the google form to the victim and collecting the information.
- The scammer gets the victim to install a remote, sharing and control application such as AnyDesk or TeamViewer. The customer then shares a 9-digit PIN, generated by the app, with the scammer. Thus, giving the scammer full access to their device.

If a victim refuses to share any information, the scammer resorts to forcing or scolding the victim, telling them it's the right way to resolve their issues.

Google form collects sensitive data including UPI PIN



The image shows a screenshot of a Google Form titled "redBus Refund Money". The form is displayed on a web browser. The URL bar shows "docs.google.com/forms/d/e/1FAIpQL5d514NpIxx14s0bWYyGjBcgh7TT45XILAI2coHT31F0K2pA/viewform". The form has a pink background. It contains the following fields:

- A description field with the text "redBus Refund Money" and a red asterisk indicating it is required.
- A "Full Name" field with a red asterisk.
- A "Mobile Number" field with a red asterisk.
- A "redBus Refund money" field with a red asterisk.
- An "ENTER UPI PIN" field with a red asterisk.

Each field has a "Your answer" label below it. At the bottom of the form is a purple "Submit" button. Below the button, there is a small text that says "Never submit passwords through Google Forms." and a footer that says "This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy".

Step 4: Activating and siphoning the victim's UPI account

The scammer collects the sensitive information to:

- Create a new UPI account if the victim does not have an account
- Activate an existing account on a different mobile number, if the victim already has a UPI account

After which, the scammers need the following details to activate the account:

- OTP for mobile number verification
- UPIACT (Example: "ACTIVATE b9a14f2312773a1f335b6b4a3e2c750e557f1d72") for physical device verification

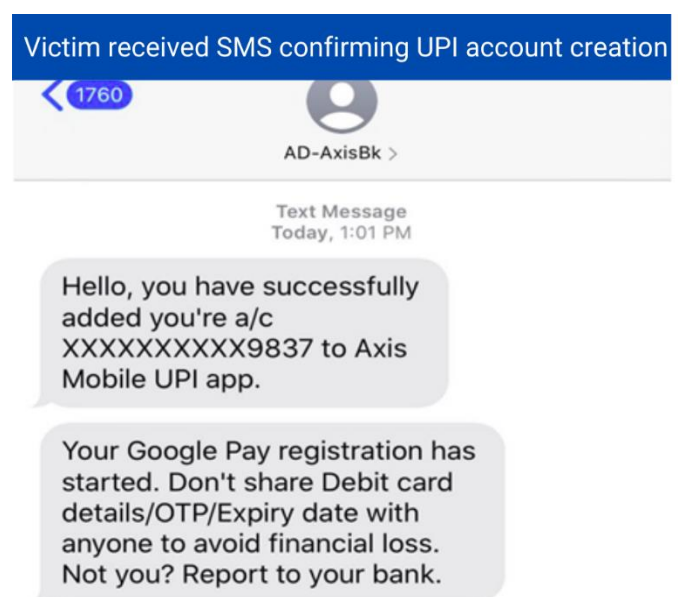
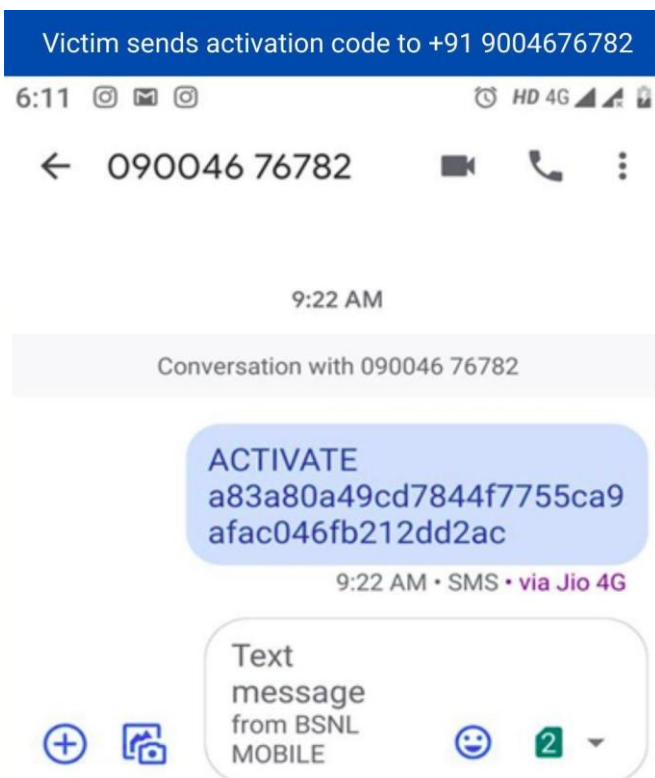
These processes of verification are crucial to create UPI accounts.

Victims are usually instructed to send these details to +91 9004676782. Once the account has been verified and activated, the scammer adds the bank account details and next the scammer uses UPI PIN collected in Step 3 or creates a new PIN using the debit card details. Interestingly, the last 6 digits of your debit card number, and the expiry date are enough to create a PIN.

To create a new PIN:

- If a victim already has a UPI account, the scammer uses the 'Forgot PIN' option and follows the instructions to reset the PIN. ([Procedure](#))
- If the victim does not have a UPI PIN, the scammer uses the victim's debit card information to create an account and set a PIN. ([Procedure](#))

Then, the siphoning begins!



Once the UPI account is activated from another device, the scammer clears the accounts through several transactions. All the while, the victim thinks his UPI was disabled or deactivated from his end.

Alternate approach

If the scammer is not successful in creating a UPI account using the above method, they call from a different number and use the following approach:

- Sometimes, scammers call victims, who are awaiting refunds from ecommerce companies, and promise to transfer the refund amount via UPI.
- The scammer then sends a UPI money request to the victim.
- The victim receives the request, along with a message that falsely claims “you have received *** amount.”
- The scammer instructs the victim to respond to the request by clicking on the “Pay” button.
- This deducts the money from the victim’s account.

Revictimizing a victim

In certain instances, scammers apologize to the victims and request them to attempt various steps in the process again, thereby revictimizing them. From time to time, victims post their experiences on various social media platforms, to which the scammers respond offering additional support. Quite often, the victims are deceived again only to be revictimized.

Firsthand accounts of people targeted by the scamming group

Case 1: [UPI fraud using Anydesk](#)



Karan Hinduja

18 February 2019

Last week, while I was on my way to the airport for my Spicejet Ltd flight, I received an automated call from the airline informing me in a very indifferent tone that my flight was cancelled. Since I made my reservation through [MakeMyTrip.com](#), I frantically started calling them as all of the airline helpline numbers were jammed. None of my calls went through, but strangely I received a very prompt call from an executive from [MakeMyTrip.com](#) to assist me. He identified himself as Deepak Verma.

After hearing me out, he assured me that he would give me a complete refund and would also go the extra mile by booking another ticket for me within 2 hours of my flight in the same price. He explained to me that there was just a hiccup, he would have to refund the money first through UPI and then only could we go ahead. He blamed the system for the long procedures and was very empathetic.

So he CONFIRMED my amount for refund, he KNEW I was travelling with an infant, my mobile number and sent me a message from [clubfactory640@gmail.com](#) with a UPIACT number. He asked me to send the code to [9004676782](#). I found it really funny and cross questioned him for 5 minutes telling him I didn't care about the refund now and that they could adjust it in the next flight but he was adamant so I sent it.

Next he asked me to download AnyDesk!!! This was the point I knew I was talking to a fraudster. Everyone knows that Anydesk is an app to remotely control another device. I immediately asked him his credentials and he gave me very valid details about Makemytrip, but I informed him I wasn't interested in the refund or the booking and that I would seek assistance elsewhere. I really thank God for the presence of mind at that moment and saving me and my family from such a grave mischance.

Also, MakemyTrip has been giving me many assurances to trace the calls but I don't think it's their cup of tea. If they couldn't keep their customers' information safe which was something within their bounds, this call trace is beyond them.

I'm writing this so we can all as a community be vigilant and not fall prey to these scams which can sometimes catch you in the most desperate times.

 328

40 comments 79 shares

Case 2: [Myntra Customer Care](#)

TanujaSood posted this 11 August 2019

06204563994 this is a mobile number of the person who is making people fool by writing on Twitter and many online platforms that this number is Myntra customer care number. This person has lotted Rs.3000 from my bank account.

I had to return a product which I bought from Myntra but I wasn't able to put return request on their website so I decided to call on their customer care number which I googled .

But after calling twice on that number my call didn't get through so I searched more n got this number from a Twitter link and it was described as myntras customer care no .

I called on this no , a guy picked up the call ,I asked him that is this Myntra no ? He said yes and then I told him about the problem I was facing regarding the return of the product.

To which he asked for the barcode of the product and the order I'd and asked in which bank do I need the refund .

I told the name of my bank and after which he said he will send me a message mobile no is (8638247958) and I need to send it to other number I.e. 9004676782 and then he will transfer the amount in my account.

I followed his instructions , after that he asked about my account number which I gave him and last 6 digits of my ATM card and expiry date of my ATM card which I gave him .(Huge mistake)

After that I received an otp number and gave him that .As soon as I did that Rs.3000 was deducted from my account .Again He asked for my full card details to which I refused.

I got suspicious and confronted him to which he said he will give my money back I just have to send a link he has sent me to which I refused coz he was tricking me again .Had I had given him the otp again he would have took more money from my bank .

When I confronted him and told him that I will file police complain he disconnected the call.

I quickly called up my bank to block my ATM card and upi I'd and filled a complaint about what happened.

But I lost Rs.3000 coz of my ignorance and blindly trusting people over phone. We get so many messages from banks and other platforms to not share our personal banking details with anyone. We should really pay attention to those messages and while dealing with money matters online and over phones we need to be very very careful.

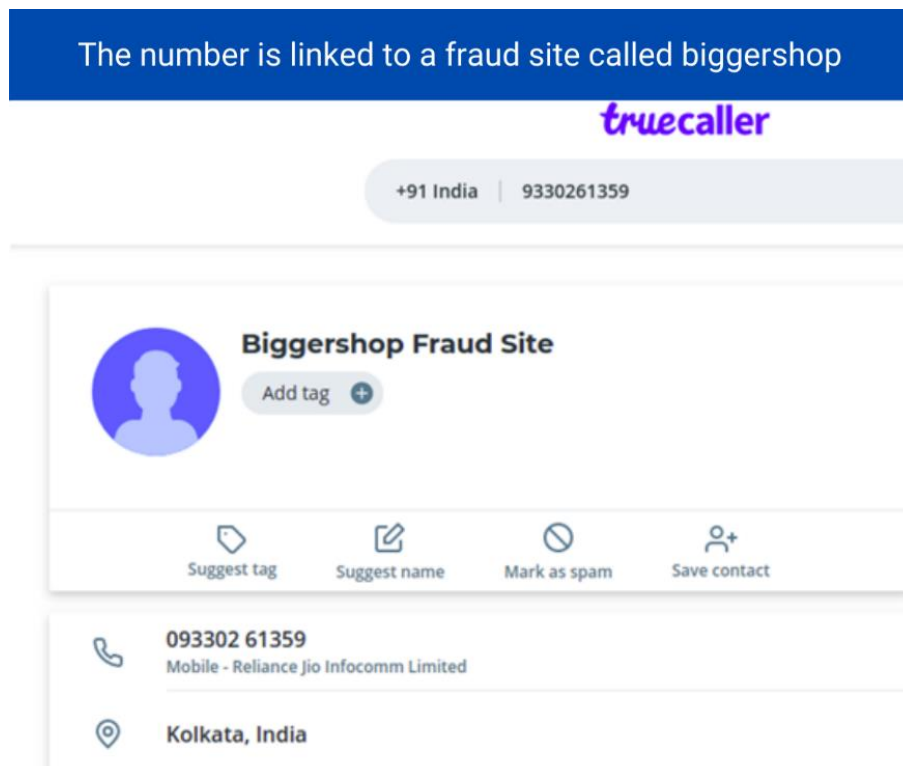
Please note this number 06204563994 this persons bank is Axis bank in Bihar it's ifsc code is UTIB0003223.

Be aware of this fraud, He seems to be decent person on phone but he is a trained hacker and in minutes will loot ur money

Who are the scammers?

By tailing the number +91 9004676782, and other numbers such as +91, +91 9330261359, +91 6204563994 that were widely associated with it, we have been able to identify several online personas of the scammers. While we may not have been able to track down every scammer associated with this group, we have identified and investigated some of these online personas individually and how they relate to each other.

On Truecaller, +91 9004676782 is linked to a fake Axis Bank customer care operation. While +91 9330261359 is used to SMS a link to the google form that collects PII & KYC information. It is also linked to a fraudulent ecommerce site thebiggershop.com. (Complete details of thebiggershop.com) Once the site was taken down, the Truecaller name linked to the phone number also changed.










thebiggershop.com


thebiggershop.com is a fraudulent website that has been created by the same scamming group to lure people with steep discounts. However, after customers have paid for items, they either don't receive the items, or receive cheap substitutes. The site does not have a customer care number, only an email id. There is no response to emails sent to this email id.

Screenshot of the archived Biggershop website

OFFER Valid Only For Today [BUY 2 GET 1 FREE] [Dismiss](#)





[HOME](#)
[SHOP](#)
[MEN](#)
[WOMENS](#)
[ABOUT US](#)
[CONTACT US](#)


Welcome to TheBiggershop Store

TheBiggershop is the global online store for designer ethnic wear. Our mission is to provide the handpicked designs of wedding sarees, designer anarkalis, lehengas, kurtis from various part of india at the best price. We guarantee 100 % authenticity of the product as it is directly sourced from the manufacturer or a licensed agent. The merchandise on our site is exclusive in nature and quantities are often limited, hence we recommend you to shop for whatever you like before it goes off the rack. We have a dedicated TheBiggershop blog to provide you to read on the latest fashion trends and keep you close to indian culture and heritage. Satisfied delighted customers is what we believe in.

TheBiggershop is the brainchild of a group of enthusiastic and dedicated fashion lovers, created with the intent to offer top-quality fashion at affordable prices. Our customers are treated to a wide range of products from well-established designer brands as well as newer but equally talented designers from all over the country



LOCATION

Unit No 1, 3rd Floor, World Trade Centre, Brigade Gateway Campus, Rajajinagar Extn, Malleshwaram(W), 560055

Email: care@thebiggershop.com

HELP

[Terms and Conditions](#)

[Shipping](#)

[Return & Exchange Policy](#)

[Order Tracking](#)

[FAQs](#)

POLICIES

[Privacy policy](#)

[Terms and Conditions](#)

[Shipping](#)


[Return & Exchange Policy](#)


COMPANY


[About Us](#)

[Contact Us](#)

Items sold on Biggershop

FREE SHIPPING WORLDWIDE 

GIVEAWAY EVERYWEEK 

SALE UP TO 70% OFF ON TUESDAY 

TRENDY CLOTHING

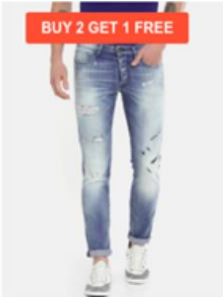
Trending

FEATURED

CLOTHING

T-SHIRTS

BUY 2 GET 1 FREE



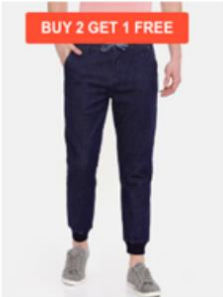
NEW-PANTS

Men Blue Glen Slim Fit Low-Rise Highly Distressed Stretchable Jeans MW33

~~Rs.1199.00~~ **Rs.359.00**

[SELECT OPTIONS](#)

BUY 2 GET 1 FREE




NEW-PANTS

Men Blue Mid-Rise Clean Look Stretchable Jogger Jeans ER56

~~Rs.1199.00~~ **Rs.359.00**

[SELECT OPTIONS](#)

BUY 2 GET 1 FREE




NEW-PANTS

Men Grey Skinny Fit Mid-Rise Mildly Distressed Stretchable Jeans TY63

~~Rs.1199.00~~ **Rs.359.00**

[SELECT OPTIONS](#)

BUY 2 GET 1 FREE



NEW-PANTS

Blue Washed Slim Tapered Fit Stretchable Jeans XM3

~~Rs.1199.00~~ **Rs.359.00**

[SELECT OPTIONS](#)

The site has been taken down, but their archived pages can be viewed here:

<http://archive.md/z6qNX>

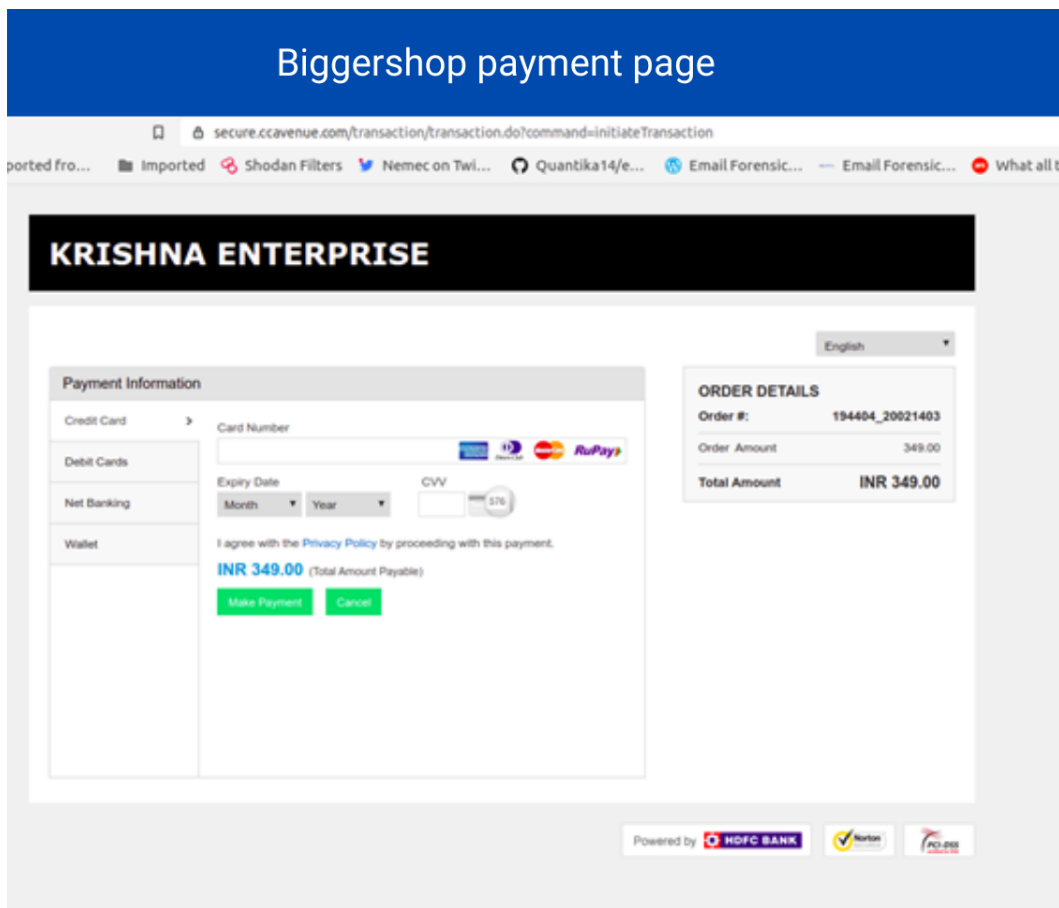
<http://archive.md/Cnp1j>

<http://archive.md/9jnvw>

Payment Details:

When a victim buys an item from thebiggershop.com, they are redirected to the ccavenue payment gateway, which is a widely used payment gateway in India. It gives customers to pay via net banking, UPI, wallets, Debit Card, Credit Card.

Merchant-Name: KRISHNA ENTERPRISE



The screenshot shows a payment page for 'Biggershop payment page' with the merchant name 'KRISHNA ENTERPRISE'. The page is powered by HDFC BANK and features logos for NetBanking, RuPay, and POB. The payment details section shows the total amount payable as INR 349.00. The order details section shows the order number 194404_20021403 and the order amount of 349.00.

ORDER DETAILS	
Order #:	194404_20021403
Order Amount	349.00
Total Amount	INR 349.00

Customer care numbers used for thebiggershop.com

These customer care numbers are used for the next phase of scam. When customers don't receive their orders, they look for thebiggershop customer care numbers. And when they call the below numbers, for refunds, the scammers collect their PII & KYC details required and siphon the victim's accounts by performing fraudulent UPI transactions.

Phone	Name and details provided by the scammers	Usage of the numbers
9064401664	Raju patal, west bengal	Thebiggershop customer care
		Ladybazaar customer care
		Google pay UPI fraud
		Bangood customer care
		Call center service
8101320217		Thebiggershop customer care
8101807298		The biggershop customer care


UPI IDs used in UPI fraud - thebiggershop refund scam:

- paytm-51091441@paytm
- paytm-51366607@paytm

Victims & Complaints

There are many users who have become victims of thebiggershop.com. Several of whom post complaints, and seek remediation, on platforms such as Facebook, Twitter, consumer complaint websites, etc., as shown below:

Complaint against Biggershop on Facebook

 **Divya Gandotra Tandon**
@divya_gandotra

I had one of my shoes on January 31, why hasn't it arrived yet.
Order no. - 72948
Email address - rajesh.reliance.kohinoor@gmail.com
Please help this is a scam shopping site. They aren't delivering anything.
[@CyberDost](#)
[#Thebiggershop](#)

Order # 72948 was placed on January 31, 2020 and is currently Processing

Order details

PRODUCT	TOTAL
SKINNY MEN'S BLUE JEANS - 30 x 1	Rs.179.50
MEN'S FASHION SHOES ACT 0106 - 7 x 1	Rs.240.50
MEN'S FASHION SHOES ACT 042 - 7 x 1	Rs.249.50
Subtotal:	Rs.669.50
Shipping:	Free Shipping
Payment method:	PayTM, UPI
Total:	Rs.669.50

Money Paid
₹ 689.50




31 JAN 2020, 01:08 pm | Closing Balance: ₹109.48

gborder
Order ID: 775b3020b4703a0b5a

Paytm Wallet
Wallet ID: 2805800201

We found the following three YouTube pages that are advertising fake customer care numbers for thebiggershop and for other legitimate e-commerce websites as well. All three videos were posted on Feb 13, and are made with videoshow. However, they have been taken down.

YouTube videos advertising Biggershop


 <p>0:12</p>	 <p>0:13</p>	 <p>0:30</p>
<p>8509293274@Saaj design customer care number 7061191047</p>	<p>8509293274@Thebig... customer care number ...</p>	<p>8509293274@Beyoung customer care number 7061191047</p>
<p>Deeraj Kumar YouTube - 1 day ago</p>	<p>Sawega Khan YouTube - 1 day ago</p>	<p>Palwi Kumari YouTube - 1 day ago</p>

We also found some people advertising thebiggershop domain link in the description section of their [Youtube videos](#). Even though the videos are not related to thebiggershop, they have similarities with the above 3 videos, in that they are made with videoshow and their audio backgrounds are similar.

YouTube account associated with Biggershop

Right leg ki mar gyi raid | devil | ""

12 views • Feb 6, 2020



DEVIL Vlogs

5 subscribers

https://thebiggershop.com/shop/mens-f...

SHOW MORE

The numbers 7061191047 & 6289849080 numbers which are advertised in thebiggershop Youtube videos: <https://twitter.com/Sahum39155170> belongs to a scammer, pretending to be a customer care executive, going by the name Ranju Kumar.

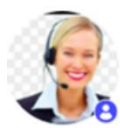
E-mail: ranjukumar6200@gmail.com

Location: Kolkata


Truecaller details of Ranju Kumar


truecaller


+91 India | 6289849080

 **Ranju Kumar**
Add tag +

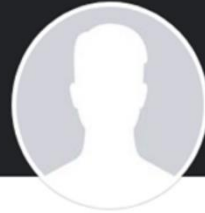
Suggest tag Suggest name Mark as spam Save contact

 **062898 49080**
Mobile - Reliance Jio Infocomm Limited

 **ranjukumar6200@gmail.com**


 **Kolkata, India**


Ranju Kumar's Facebook account



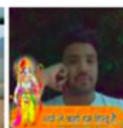
 **Ranju Kumar**
Timeline About




DO YOU KNOW RANJU?

To see what he shares with friends, send him a friend request

 Photos


 Friends · 10

 Sunny Sarkar
  Kaushik Kumar
  निशु मिश्रा


 Lakhinder Thakur
  Madan Mahato
  Emraan Ali

The scammer is seen advertising the number +91 7061191047 as customer care number for other companies such as Kytary and Radiant International. Of which, Radiant International is a fake company, whose website has been taken down.

Ranju Kumar advertising fake customer care numbers on Facebook

 **Ranju Kumar** ▶ **Kytary**

Jan 30 · 🌐 · Kytary customer care number 8509293274+7061191047Kytary customer care number 8509293274+7061191047Kytary customer care number 8509293274+7061191047Kytary customer care number 8509293274+7061191047

 **Ranju Kumar** ▶ **Radiant International**

Feb 2 · 🌐 · ...number 8509293274Radiantinternational express customer care number 8509293274

While Ranju Kumar's profile details are not available, we can understand the scammer, by investigating his friends, who could also be scammers.

Ranju Kumar's friends

- <https://www.facebook.com/profile.php?id=100023568649641>
- <https://www.facebook.com/profile.php?id=100002602175592>
- <https://www.facebook.com/contact2ibm>
- <https://www.facebook.com/profile.php?id=100010441154631>
- <https://www.facebook.com/madan.mahato.718>
- <https://www.facebook.com/profile.php?id=100039979291038>
- <https://www.facebook.com/sunny.sarkar.7165>
- <https://www.facebook.com/nishi.mishra.758>
- <https://www.facebook.com/lakhindar.thakur.984>

UPI ID:

8609415059@airtel - Pratima Haldar

UPI Names:

Rakesh Mishra (Gurgaon)

Mukesh Singh

Abhishek Sharma

Sri. Manish Kumar

Threat Actors Social Media Presence:

- Khusbun: <https://www.reddit.com/user/khusbun/>
- Kanil: <https://twitter.com/Kanil60546809>
- Ranju Kumar: <https://www.facebook.com/ranju.kumar.90281943>

- ◆ <https://www.facebook.com/pg/radiantinter>
- ◆ Friends of Ranju Kumar
- ◆ **Kopn Kumar:**
 - https://www.youtube.com/channel/UCpKFEfr7LSvGbVgPX_8OQ1A

- **Rubelali:** <https://twitter.com/Rubelal01828634>
- <linkedin.com/in/arrival-fit-b5b503194/>
- Samima <https://nojoto.com/profile/02d7e769c2713af2ad9b5d37ab922cb6/samima>
- Imam khan: <https://www.yourquote.in/imam-khan-bukp8/quotes>
- Imam: <https://nojoto.com/profile/6e0a14599033a9efa06c404d91a7e957/imam>
- Sheherkiladki: <https://www.linkedin.com/in/sheherkiladki-customer-care-number-8ba37a186/>
- <linkedin.com/in/arrival-fit-b5b503194/>

Other businesses owned by the scamming group:

Cheap Fair

The phone number advertised in the below website is also one of the scamming number mostly used by the scammers 7439020078 explain about the website a little.

Website	https://cheappfair.com/hotels/
Archived Page:	http://archive.md/wip/N6c48
Complaint	https://www.consumercomplaintonline.in/company/frenchcrown-customer-care-complaint-number-714
Google UID	105649975601906394431
Google Analytics ID(fake)	UA-52447-2
Twitter post sharing numbers	https://twitter.com/Kanil60546809/status/1209827919196872704

Fake Customer Care Website

<https://5c6508a9dc038.site123.me/>

Club Factory-Fake Website

Website	https://traveltrivagoorefundcontactus.wordpress.com/
E-mail	clubfactory640@gmail.com
Google UID	105649975601906394431
Google Analytics ID(fake)	UA-52447-2
Twitter post sharing numbers	https://twitter.com/Kanil60546809/status/1209827919196872704

How to avoid becoming victims of this group?

- Check if the customer care numbers are official ones. And get the numbers from official websites instead of blogs or social media.
- Do not trust Truecaller data all the time.
- Don't post sensitive details or complaints on social media. Use official communication channels to address complaints against your service provider.
- Don't share your debit card details, credit card details, or KYC details through google forms. Banks never ask for such details.
- Treat your M-PIN or UPI PIN exactly like you treat your ATM PIN. Do not disclose or share it with anybody.
- The same applies for UPI login passcode – a password that you need to enter to log in to your UPI app.
- If someone sends you an unwanted money request on your UPI app, there is nothing to worry about. You can simply decline it. The amount will not be deducted from your account unless you accept the request and enter your M-PIN.
- When it comes to AnyDesk remote sharing and control app, the RBI says: "Fraudsters may ask you to download AnyDesk App and share a 9-digit code which gets them access to your phone to steal money. Any Desk is capable of acquiring full access to your smartphone remotely and would let fraudsters carry out banking transactions remotely."

Appendix

Thebiggershop.com details

Whois Details:

Whois details are protected by whoisguard. Hence only the following details are available:

Website	https://thebiggershop.com/
IP	167.99.65.178 (digital ocean)
Registration Date	October 04, 2019
Expiry Date	October 04, 2020

DNS Records:

MX	mx1.privateemail.com
-----------	--

Contact details

E-mail	care@thebiggershop.com
Facebook	https://www.facebook.com/TheBiggerShop/
Facebook	https://www.facebook.com/thebiiggershop/ (Started on January 10)
Instagram	https://www.instagram.com/thebiggershop/
Google Analytics ID:	UA-156370835-1

Technology Stack - Thebiggershop:

Cpanel	Wordpress v5.3.2
Wordpress Plugins	WooCommerce 3.9.0
	Contact Form 7
	Mailchimp
Hosting Panel	EasyEnginev4.0.14
Database	MySQL
CDN	Cloudflare
Other	PHP,Bootstrap,Docker

Archived Pages:

<http://archive.md/z6qNX>

<http://archive.md/Cnp1j>

<http://archive.md/9jnvw>