

An Analysis of the Fake Customer Care Numbers In India

Author: Vikas Kundu

Co-Author: Hansika Saxena

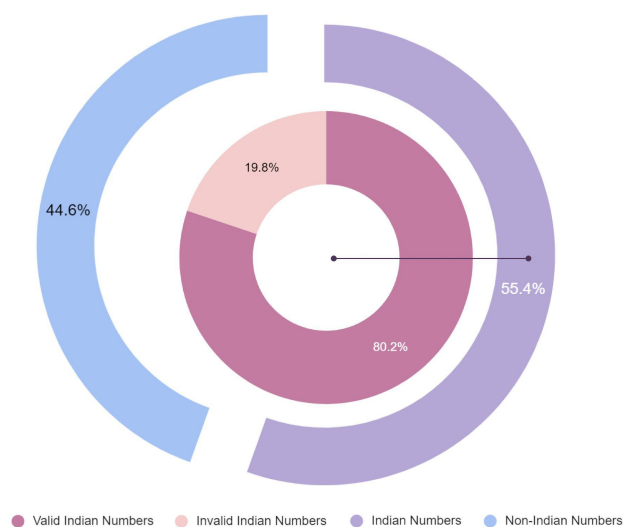
Table of Contents

Table of Contents	1
Introduction	2
How Fake Customer Care Scams Work?	3
States-wise Distribution of Fake Customer Care Numbers	3
Most Targeted Industries	4
Logo-Based Breakdown of Impersonated Entities	5
Content-Based Breakdown of Impersonated Entities	5
Channels Exploited to Disseminate the Fake Numbers	7
Social Platforms Abused for Maximizing Campaign Potential	8
The Transient Existence of Fake Numbers	9
Analyzing the Top Three Fake Customer Care Numbers Detected	10
Timing Duration & Frequency of the Scam Calls	11
Conclusion	12
Attribution	12
About CloudSEK	12
Appendix	13

Introduction

Customer service is at the crux of any marketing strategy. When customers are deadlocked with any issue, the first instinct is to contact the customer service department. These intentions are met with a resolution to the problems they face.

Today fraudsters are cashing in on the gullibility of anxious customers who reach out to the customer service department of an entity. Fake customer service calling numbers are set up to deceive customers who face product queries. This is an apt modern-day phishing technique, which builds around the trust created in solving customer queries. There have been instances where [a customer lost as much as Rs. 16,00,000](#) due to a wrong google search leading to a fake customer care number.

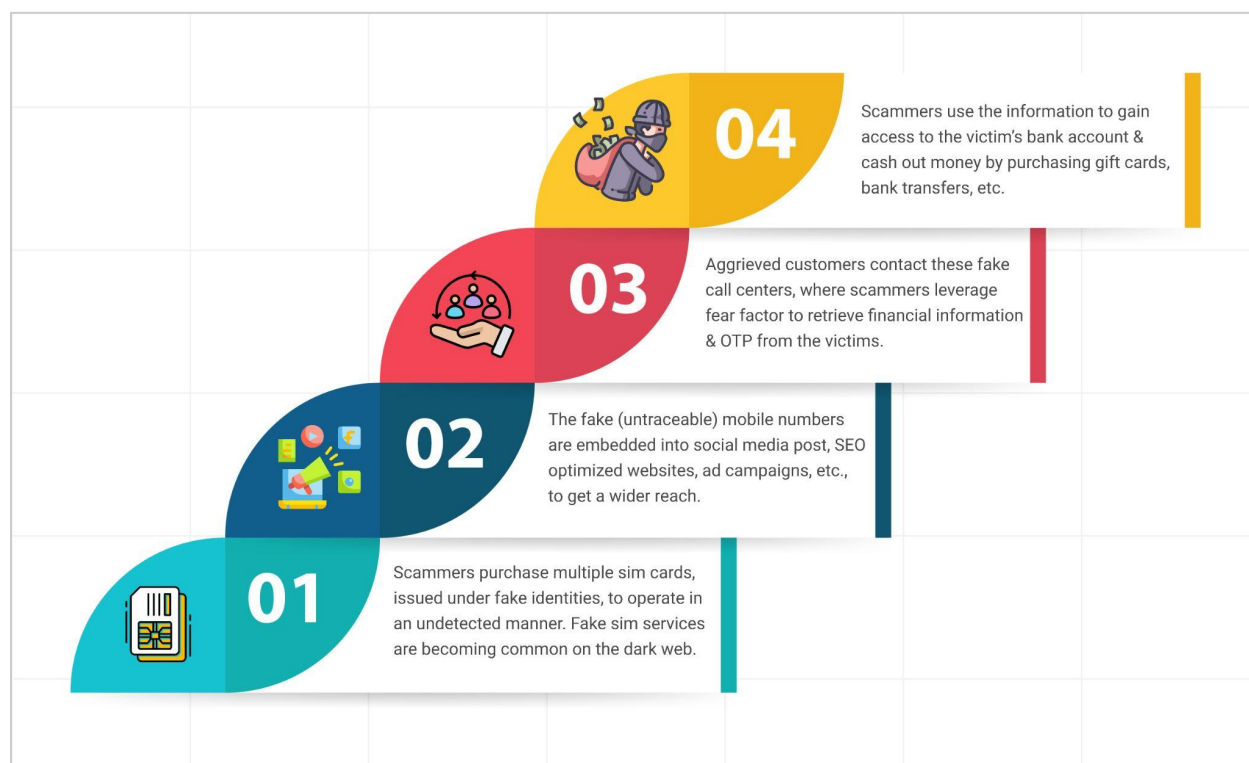


Fake customer care numbers have been thriving under the cyber radar purely because people tend to be ignorant while engaging with customer care numbers. XVigil's Fake Customer Care module has flagged 31,179 such fraudulent numbers (some of which have been active for over 2 years). The findings show that:

- ~56% (i.e. 17,285) of these were Indian numbers, while the rest were non-Indian.
- 80% of the Indian numbers were found to be valid and still operational

XVigil's Fake Customer Care Number module scours the internet for fake customer care numbers. In this report, CloudSEK researchers have analyzed a sample of **~20,000 Indian mobile numbers** used by threat actors, to run such customer care scams. As the data shows, none of the major telecom carriers, which have vast network connectivity, have been spared by scammers.

How Fake Customer Care Scams Work?



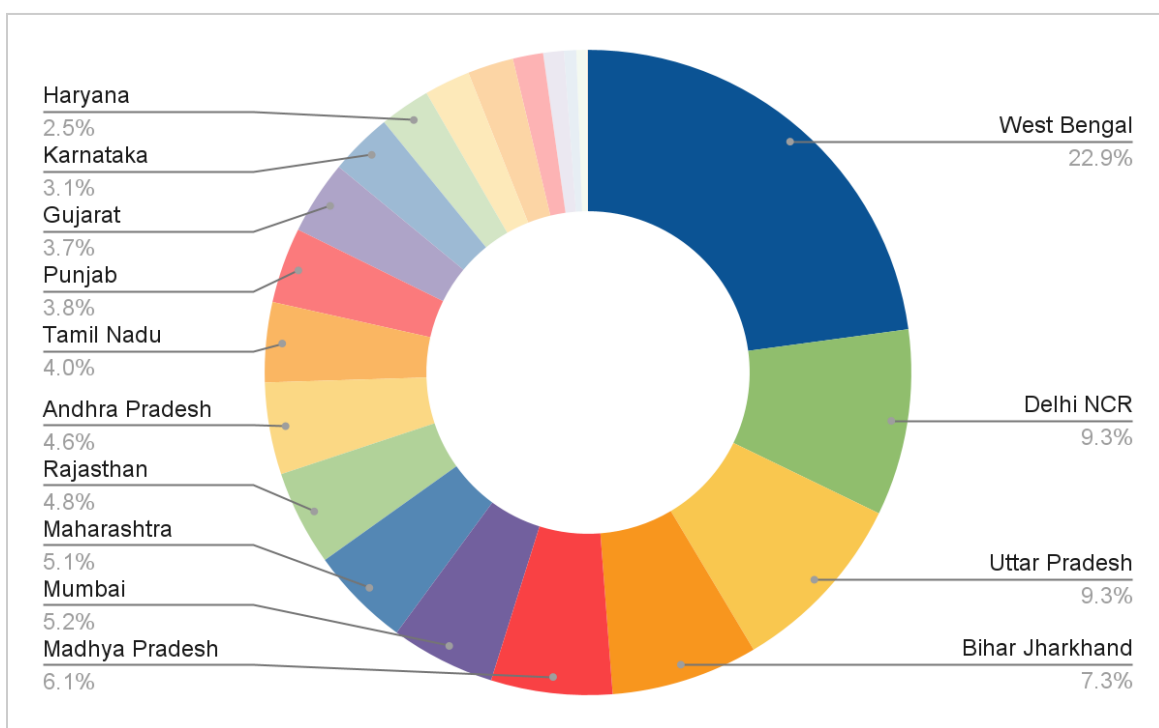
Graph depicting the steps involved in scamming users via fake customer care numbers

The working of these scams has been more or less the same over the years where the scam begins with the purchase of burner (untraceable) sim cards. These sim cards are issued under fake identities and allow the threat actor to operate without worry. Threat actors are increasingly using this modus operandi to remain undetected. As a next step, they use social media posts, websites with search engine optimization techniques, and advertisements to get a wider reach and be accessible on search engines. The unwary users search for them and may end up calling a fake customer care number. When customers call these fake call centers, they use this opportunity to retrieve financial information, OTP, etc., from aggrieved customers via social engineering methods. Generally, scammers try to leverage impersonation and the fear factor to collect money from the victims. Thereafter, the threat actors gain access to the victim's bank account and purchase gift cards, etc, or transfer the amount to another account.

States-wise Distribution of Fake Customer Care Numbers

An analysis of the area-wise breakdown of fake numbers revealed **West Bengal** as the most prominent hub, accounting for **~23%** of the total registered fake customer care numbers. Kolkata served as the center for many large-scale operations. **Delhi and Uttar Pradesh** tied up for the second place, accounting for **~19%** of the total registered fake numbers (9.3% recorded in each state). A possible reason for this can be the presence of various fake SIM card rackets in [West Bengal](#), [Delhi](#), and [Uttar Pradesh](#). Law enforcement in these regions has time and again busted several groups with SIM cards purchased using stolen or forged identification documents.

Other major cities account for a meager fraction of the total number of fake customer care numbers. It is important to note that **while the numbers are registered in these regions, they may be used from different locations to target victims across India.**



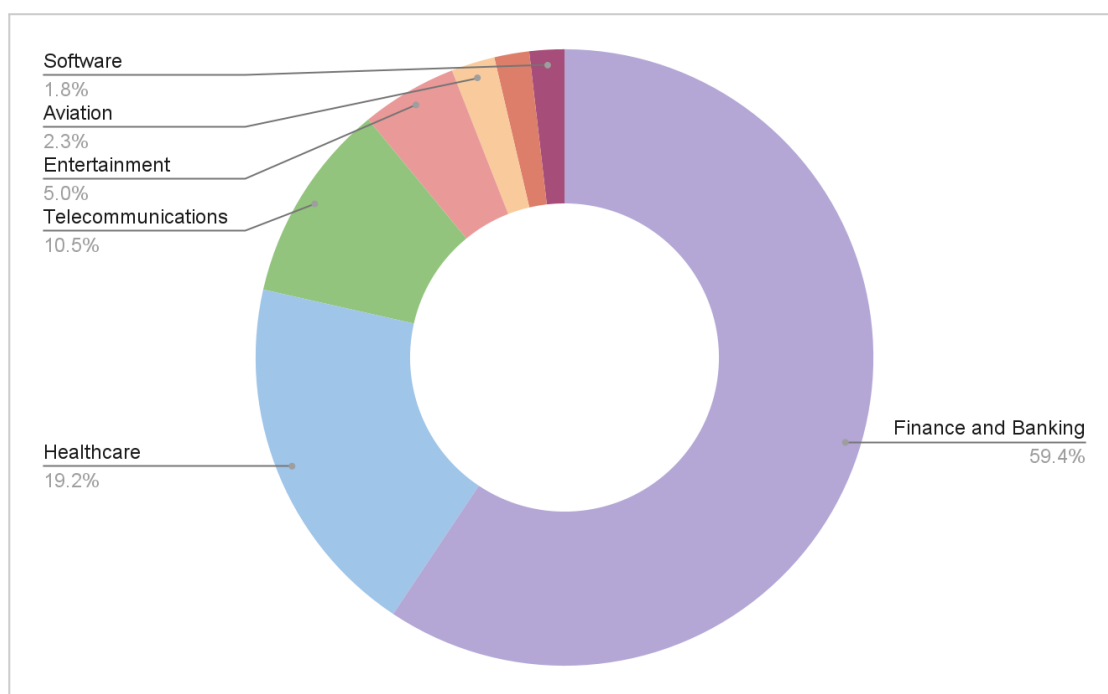
Area-wise breakdown of Fake Customer Care numbers

Most Targeted Industries

In an attempt to deceive unsuspecting users, scammers utilized various means to impersonate genuine entities, including their **name, logo, and similar-sounding domains**. Identifying the entities targeted by these fake numbers proved to be a challenging task. While some could be identified through profile images in Truecaller records, others required a more in-depth analysis of the content on the associated source domains.

Logo-Based Breakdown of Impersonated Entities

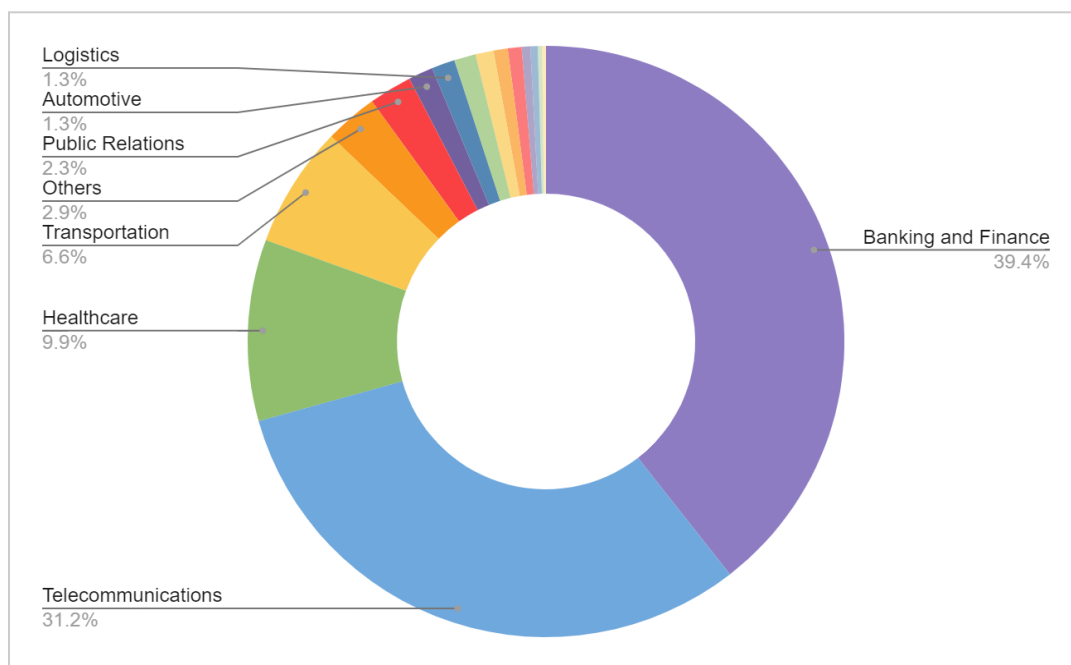
Logos from the images present on the Truecaller IDs, helped identify and categorize the extent of the threat across various industries. Our analysis revealed that the **Banking and Finance** sector was the most targeted industry, followed by **Healthcare, Telecommunications, and Entertainment**.



Industry-wise breakdown of logos impersonated by scammers

Content-Based Breakdown of Impersonated Entities

Analysis of the content present on the source domains associated with each number showed that entities in the **Banking and Finance** sector were the primary targets of impersonation, followed by those in the **Telecommunications and Healthcare** sectors.

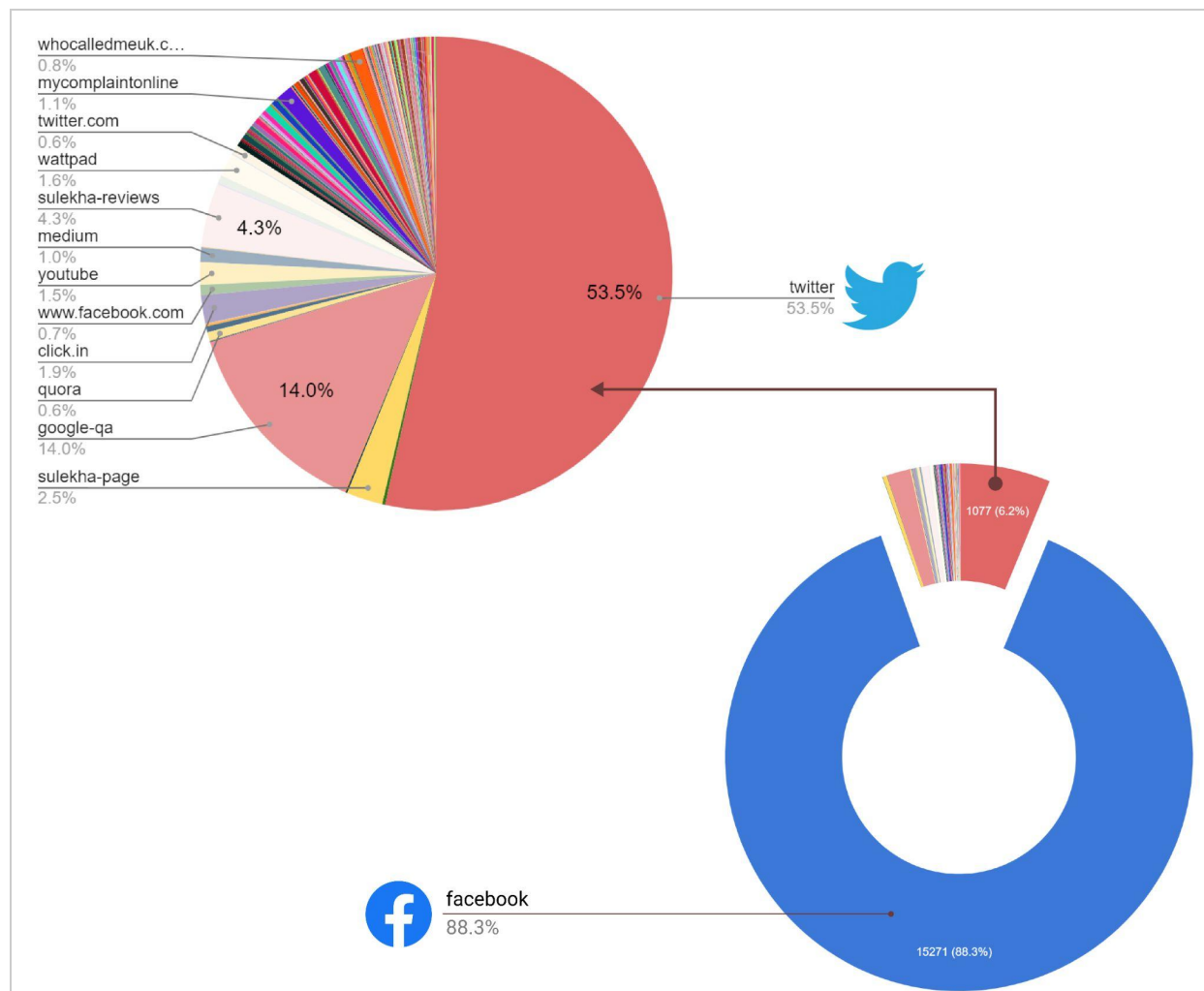


Industry-wise breakdown of entities targeted via content by scammers

Channels Exploited to Disseminate the Fake Numbers

88% (15,271) of the fake customer care numbers were distributed via **Facebook** advertisements, posts, profiles, and pages. Out of the remaining 12% of the numbers, **Twitter** emerged as the most popular distribution medium, accounting for 53% of the traffic (6.2% of the total traffic). Twitter was followed by Google which was responsible for 14% of the remaining traffic.

Despite [Facebook claiming to have taken down close to 2 billion fake accounts per quarter](#), scammers continue to flood Facebook with fake profiles and pages. Social media continues to be the preferred medium for scammers to trick people because it allows them to reach a large user base in a short period.

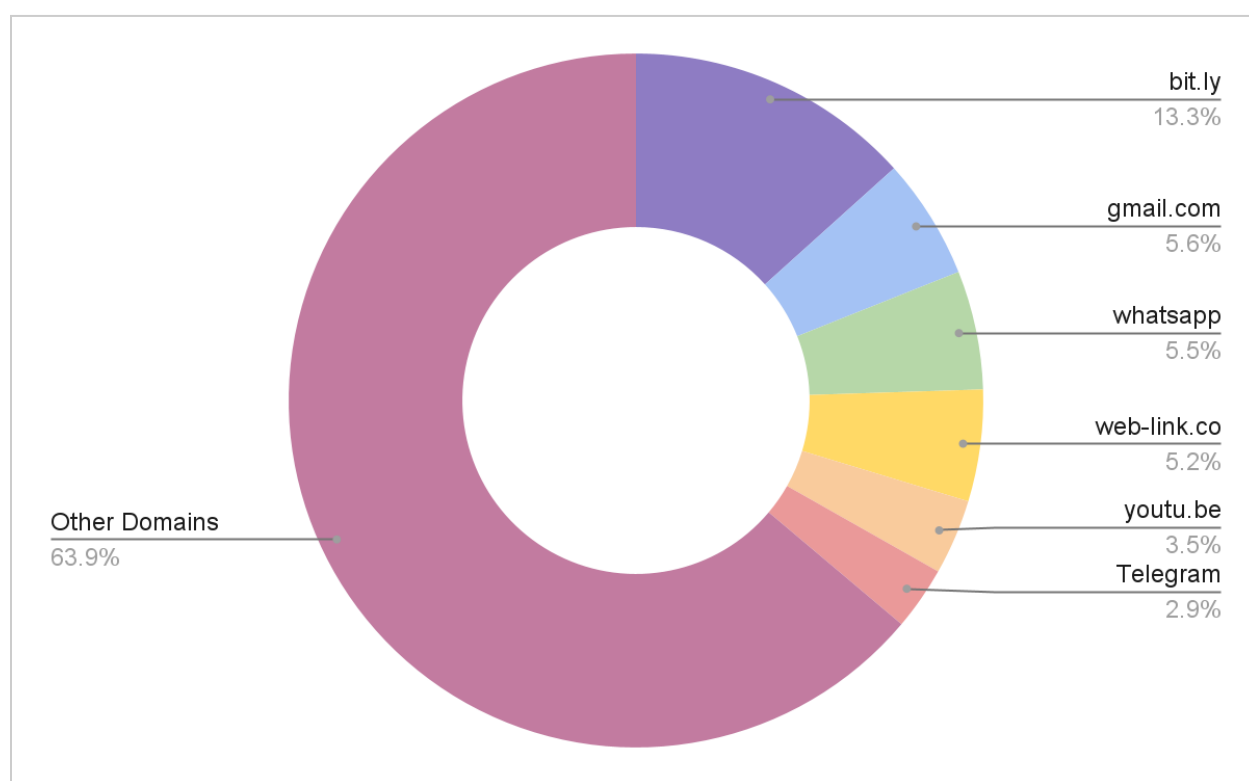


Breakdown of Sources Utilized to Spread Fake Customer Care Numbers

Social Platforms Abused for Maximizing Campaign Potential

To create an impression of authenticity, scammers frequently include a brief introduction and links to their social media accounts or posts alongside the counterfeit customer support numbers. However, a closer examination of these links reveals that they typically lead users to fake domains, fraudulent Whatsapp or Telegram accounts, and sometimes even fake email addresses. Scammers leverage social media accounts to lure customers to:

- Call on fake customer numbers
- Visit phishing sites
- Send emails from their personal accounts, thus compromising their email IDs



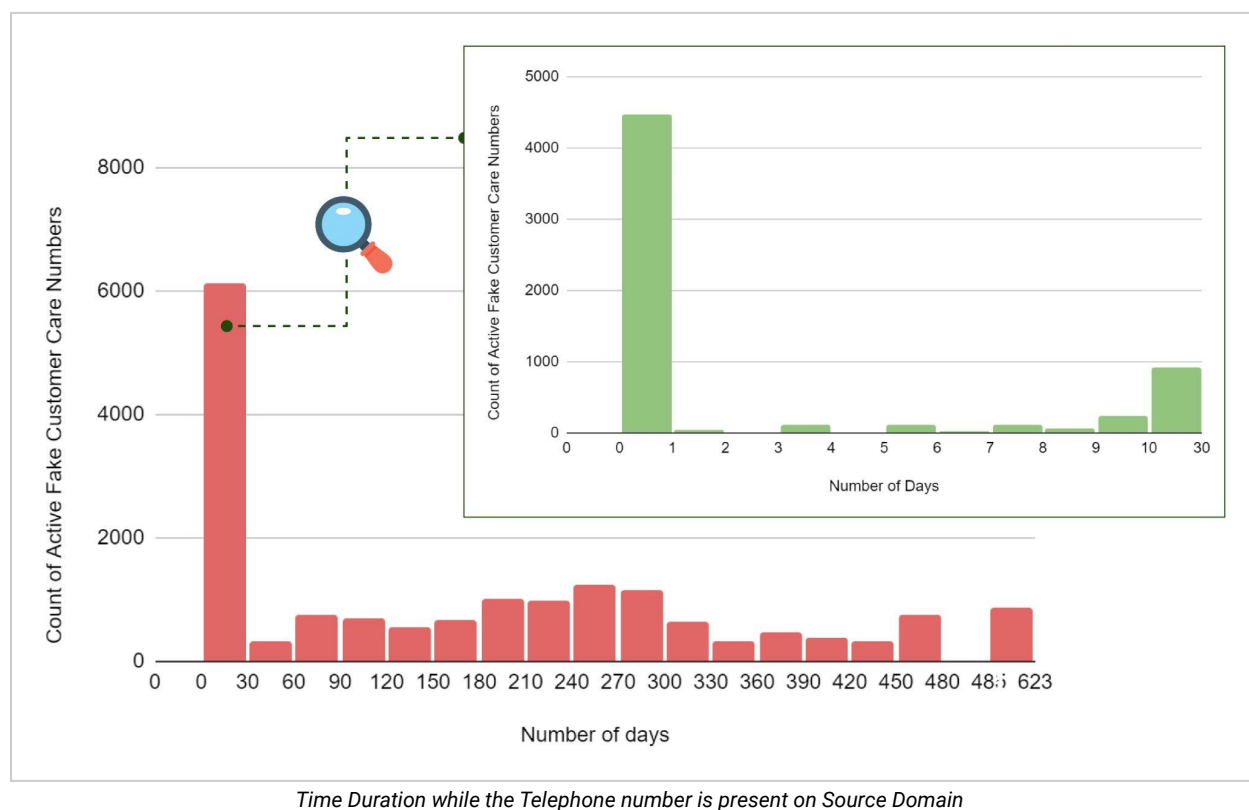
Breakdown of Sources within the content on social media posts

In order to deceive users, scammers employ a variety of tactics, such as:

- Using URL shortening services like **bit.ly** and **web-link.co** (13.3% and 5.2% respectively) to redirect victims to scam websites.
- Additionally, fake Gmail accounts were used as a means of contact for customers in need and accounted for ~5.6% of posts.
- Whatsapp was the most commonly used messaging service, followed by Telegram.

The Transient Nature of Fake Numbers

XVigil analysis revealed that a substantial portion of these telephone numbers (6,118) had a transient presence on the source domain, lasting no longer than a month (30 days). Despite this, some fraudulent numbers (881) managed to maintain their content on the source domain for a period ranging between 485-623 days. This finding suggests that **while some scammers were implementing sophisticated tactics to evade detection and prevent their content from being taken down from the source domain, others were shifting source domains frequently.**



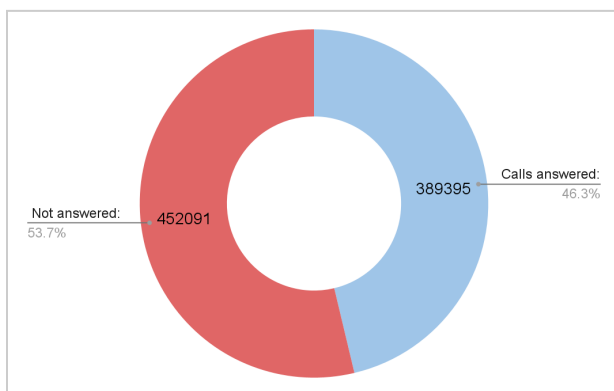
Upon closer examination of the data, it was observed that during the span of a month, the majority of the numbers (4,470) appeared only once. Despite this, a significant proportion of these numbers remain active and around **290 of them flagged as spam** based on data obtained from TrueCaller. As many of these numbers were associated with posts on Facebook, it is probable that the social media platform utilized its machine learning algorithms to remove the content or that the scammers changed their approach and began targeting users through alternative sources after their activities were detected.

Analyzing the Top Three Fake Customer Care Numbers Detected

The following three numbers were seen impersonating top Indian Banking and Finance firms and were operational roughly for a period of more than 600 days.

Fake Number	Details
+918116494943	<ul style="list-style-type: none">• Name on TrueCaller: Avinash Kumar• Brands Impersonated: Fashion and BFSI entities• Discovery source: Sulekha• Location: West Bengal• Additional Info:<ul style="list-style-type: none">○ 356 search results were found on TrueCaller for “TOP SPAMMERS”.○ Google search for the number suggests that it was targeting multiple Finance and Banking entities. (Images added in Appendix)
+917001088584	<ul style="list-style-type: none">• Name on TrueCaller: Sipahi Sahni• Brands Impersonated: BFSI entities• Discovery source: Twitter• Location: West Bengal• Additional Info:<ul style="list-style-type: none">○ Targeting multiple Finance and Banking entities via Twitter account. (Images added in Appendix)○ TrueCaller ID of the number contains the logo of a prominent Indian bank.
+918697355745	<ul style="list-style-type: none">• Name on TrueCaller: Mitra Pvt Ltd• Brands Impersonated: BFSI entities• Discovery source: Facebook• Location: West Bengal• Additional Info:<ul style="list-style-type: none">○ TrueCaller ID of the number contains the logo of Bank Mitra. (Images added in Appendix)

Timing Duration & Frequency of the Scam Calls

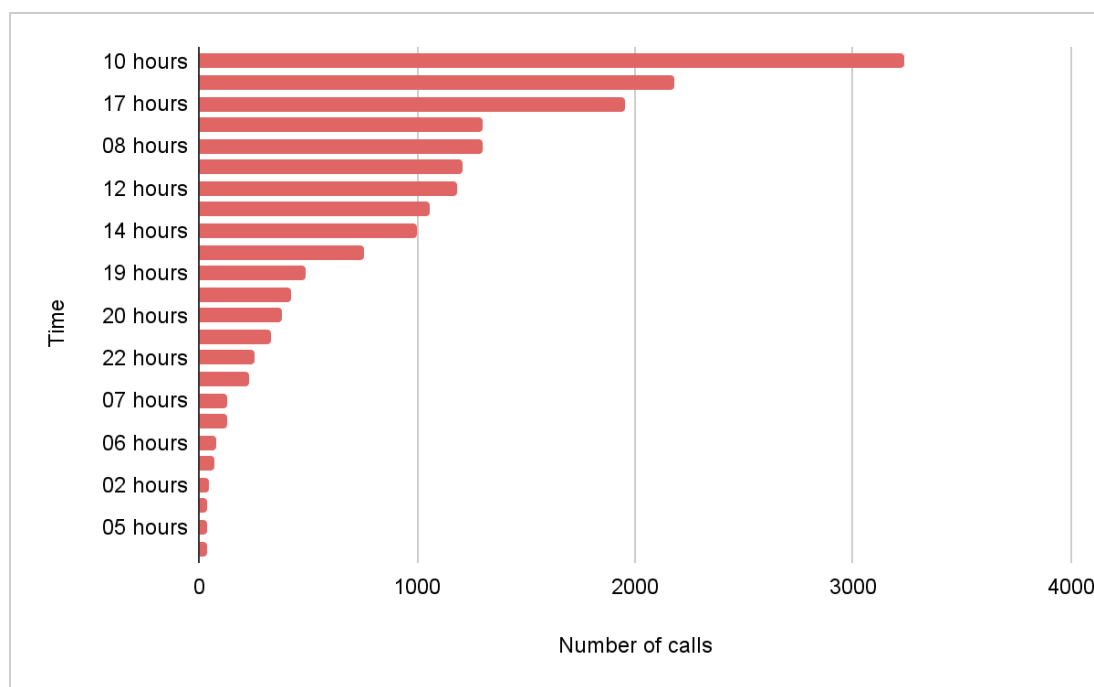


Frequency of scam calls answered v/s not answered

During the analysis of 841,486 calls (made from 470 numbers), it was found that ~47% of the calls were answered by innocent individuals, and some of these numbers were later used by scammers to make direct calls. Consequently, these calls were flagged as **spam** by TrueCaller. XVigil was able to identify a total of 1,490 such fake numbers. Interestingly, out of the 1,490 flagged numbers, 470 contained intricate details

about the precise timing of the calls made within the last 60 days.

Analysis of these 470 numbers reveals that the preferred calling time for scammers targeting Indian citizens was 10 AM in the morning, followed by 5 PM in the evening. The 46.3% success rate of the spam calls (i.e. answered calls) amounts to an **average of 30 calls per day being made from a single number**. It is interesting to note that apart from India, **214 calls** were made to Dubai from these numbers in the last 60 days.



Number of calls v/s the timing durations of the scam calls

Conclusion

Customer care is an essential part of any successful business that consumers rely on for quick resolution to the issues they are facing. The importance of customer care and consumers' urgency for resolution makes it an attractive target for threat actors and scammers. Companies need to actively educate customers on legitimate sources and means to reach their customer care services. It is also important for businesses and consumers to report suspicious numbers and work with authorities to get them flagged or taken down.

Attribution

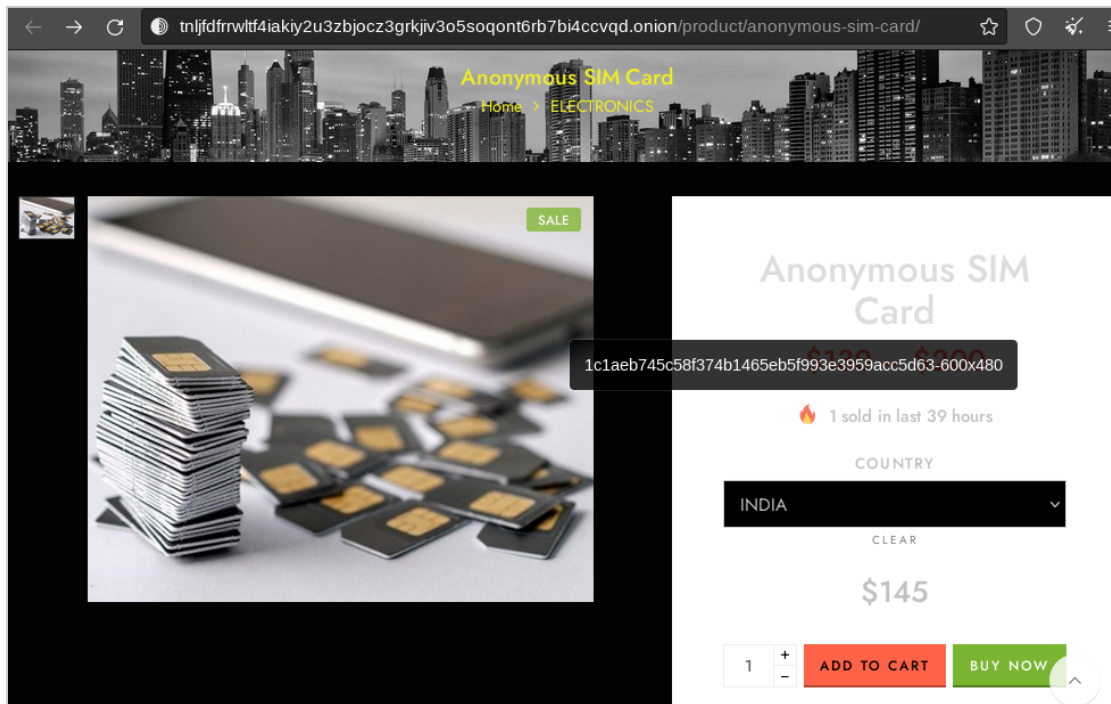
- [Four step process infographics](#)
- [Icon used in infographic](#)
- [Icon used in infographic](#)
- [Icon used in infographic](#)
- [Icon used in infographic](#)
- [Icon used in infographic](#)

About CloudSEK

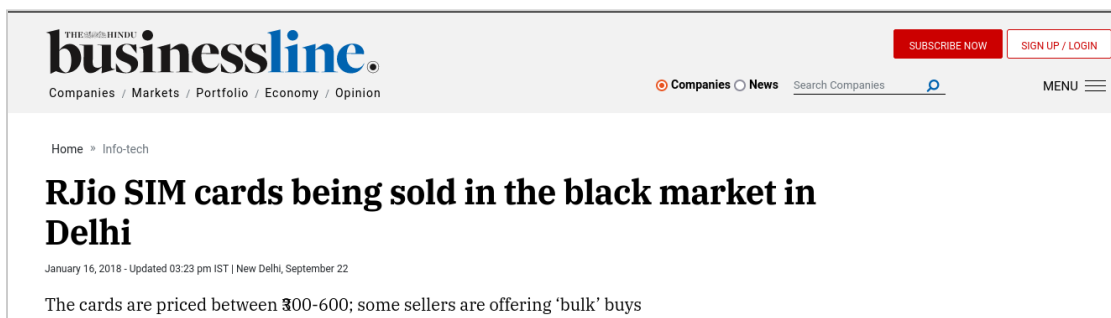
CloudSEK is a contextual AI company that predicts Cyber Threats. Our Cloud SaaS platform constantly seeks security solutions for our customers' digital risks.

To learn more about how CloudSEK can strengthen your external security posture and deliver value from Day One, visit <https://cloudsek.com/> or drop a note to info@cloudsek.com.

Appendix




Fake sim cards are being sold on a dark web website



Incident of fake sim cards being sold illegally




Incident of fake sim cards being sold illegally


G.pay (Tezz) App Customer Care | Any Payment Problems Call Now |... 

Ad googlepaycustomercarehelpline.blogspot.co...

Call Now Get G.pay App Online Solutions. We Solve Tezz (G.Pay) App Online Payments And Account Creation Problems. 6370569305. 6289204301. 7070011014. 6205565778.

 **Call 062893 77355**

Fake customer care number embedded in a Google advertisement

 <https://bankscustomercarenumbers.blogspot.com/2014/02/canara-bank-customer-care-toll-free.ht>

← **Bank Customer care number|customer care numbers|all banks c**

Anonymous 5 July 2018 at 08:30

CANARA BANK CUSTOMER CARE HELPLINE NUMBER FOR ANY PROBLEM ANY QUESTION CONTACT TO HELPLINE NUMBER

6204705981....7358802484...7416871723

CANARA BANK CUSTOMER CARE HELPLINE NUMBER FOR ANY PROBLEM ANY QUESTION CONTACT TO HELPLINE NUMBER

6204705981....7358802484...7416871723

CANARA BANK CUSTOMER CARE HELPLINE NUMBER FOR ANY PROBLEM ANY QUESTION CONTACT TO HELPLINE NUMBER

6204705981....7358802484...7416871723

CANARA BANK CUSTOMER CARE HELPLINE NUMBER FOR ANY PROBLEM ANY QUESTION CONTACT TO HELPLINE NUMBER

6204705981....7358802484...7416871723

CANARA BANK CUSTOMER CARE HELPLINE NUMBER FOR ANY PROBLEM ANY QUESTION CONTACT TO HELPLINE NUMBER

6204705981....7358802484...7416871723

CANARA BANK CUSTOMER CARE HELPLINE NUMBER FOR ANY PROBLEM ANY QUESTION CONTACT TO HELPLINE NUMBER

6204705981....7358802484...7416871723

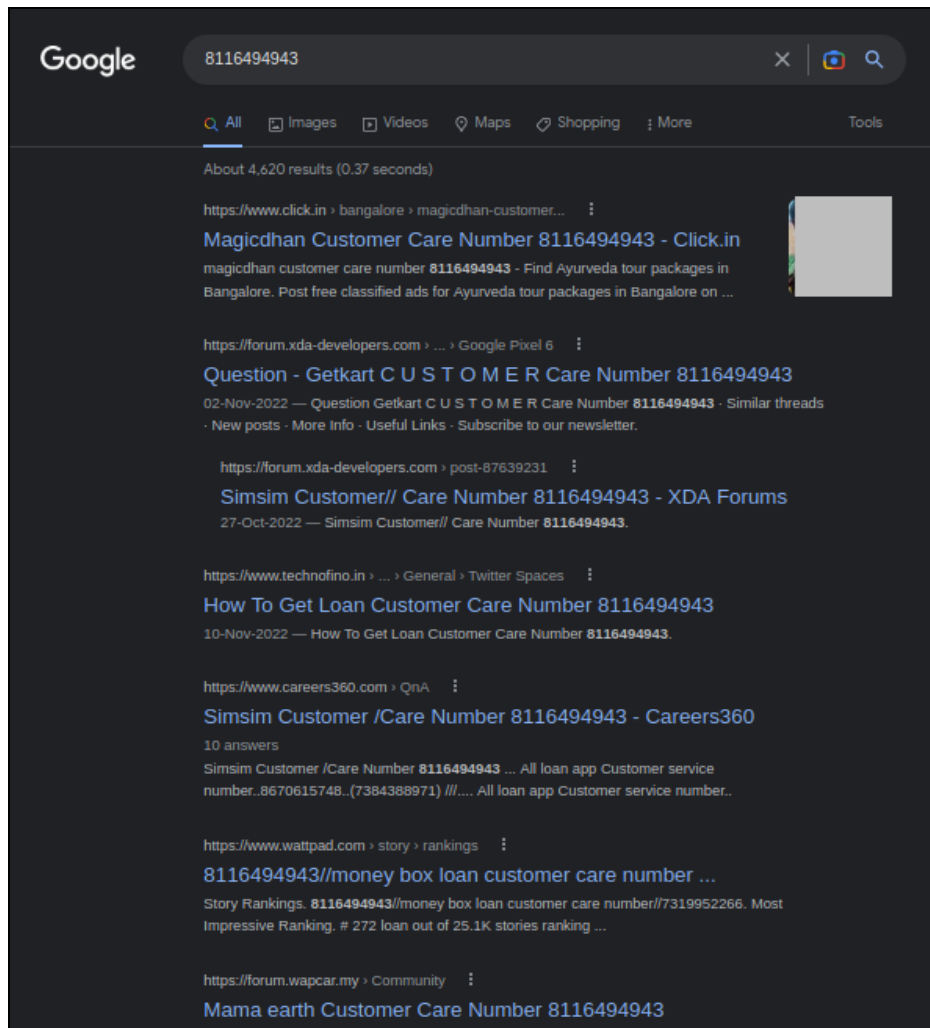
A website embedded with fake customer care numbers



Fake customer care number targeting multiple entities



Logo of a Fake customer care number on Truecaller



Fake customer care number targeting multiple entities