Paytm's Response to TRAI Consultation Paper on Leveraging Artificial Intelligence and Big Data in Telecommunications Sector

1. Introduction:

At the outset, we are thankful to TRAI for initiating this consultation paper and according opportunity to all stakeholders to present their views regarding commissioning and adoption of Artificial Intelligence and Big Data applications in the Telecommunication ecosystem.

Paytm is India's largest financial services platform with over 75 million monthly transacting users and 28 million merchants on its platform as of June 30, 2021. As per TRAI's subscriber data of June 2022[1], there are about 801 million broadband Internet subscriber in India out of which only a meagre 29 million subscribers (3.62%) are wireline broadband Internet. This is a clear indication that about 96% of Internet users accesses various applications and services over the cellular network. The Fintech and Financial Services industry is no exception, as this ecosystem too relies significantly on wireless telecom service providers (hereinafter referred to as TSPs) to deliver seamless and secure financial services and products to end consumers.

The present consultation paper is a welcome and timely initiative and we are pleased to note that TRAI has taken cognizance of the fact that Artificial Intelligence and Big Data applications on the telecommunication network can play a pivotal role in securing network access for edge applications. Even though the present consultation paper does not raise specific questions regarding role AI can play for financial security, we would like to take the liberty to submit our response with regard to issues that are specific to the financial services / Fintech ecosystem.

Increasing smartphone usage throughout the world has accounted for large amounts of data being shared through digital means. Customers are required to fill in their personal information through online banking apps and also need their phone numbers to complete various everyday tasks that involve financial transactions (for e.g E-Commerce, banking transactions, E-Governance transactions like paying taxes, challans etc.). Meanwhile, the telecom industry continues to face concerns due to fraudulent activities like SIM swap fraud and data theft, both of which arise due to the lack of identity verification. Even though there have been developments in the form of remote operations, the industry is still not free of identity fraud and financial crime. Mobile devices that are used for making online transactions and communicating sensitive information are vulnerable to fraudulent activities. Even the smallest of loopholes in a mobile network can enable fraudsters to use smartphones for identity fraud, payment scams, and account takeover.

[1] https://www.trai.gov.in/sites/default/files/PR_No.53of2022_0.pdf

Fraudulent methods like SIM Boxes are now being adopted by scammers to capitalize on free SMS bundled with tariff plans. Using this method, fraudsters take payments and send SMS messages to thousands of random recipients to try and obtain personal information. If successful, they use the personal information for SIM swaps, which itself is a kind of identity theft targeting a mobile phone to get access to social media accounts, bank accounts, and even crypto wallets by getting their hands on OTPs (one-time passwords).

SIM swapping fraud isn't the end of the story, as phishing SMS techniques are also seen targeting telecommunication companies here and there. While SIM swapping remains an easy task for fraudsters, it has negative effects on both telcos and their customers. In the absence of regulatory measures that require robust identity verification measures, the industry will see increasing fraud rates in the years to come.

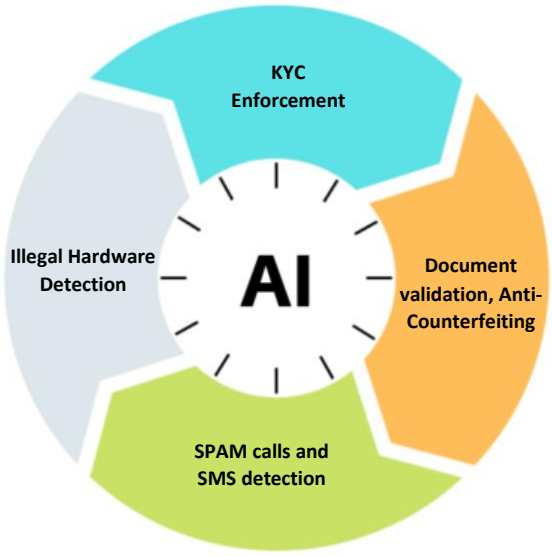

Figure 1: AI Impact Areas for Fintech Security

We would like to take this opportunity to submit our responses and recommendations to specific issues highlighted in the present consultation paper, as discussed in the following section:

2. SPECIFIC SUBMISSIONS:

I. AI Applications for KYC management and enforcement:

Artificial intelligence (AI) is poised to improve security across the telecommunication landscape as rightly highlighted in the consultation paper. From AI-powered surveillance to automated data extraction, AI technologies are optimizing security efforts for telecommunication and financial institutions. AI development services are set to disrupt legacy processes like Know Your Customer or KYC for improved verification and enhanced customer experience. AI development for KYC deploys technologies like computer vision, Natural Language Processing (NLP), and machine learning for significant value generation.

While banks and financial institutions have already deployed such systems in varying degrees and architectures, telecommunication service providers can also evaluate and implement AI driven processes for automating KYC.

The traditional KYC process is laden with multiple layers of verification stages, both manual and digital. The process begins with the collection of data from millions of customers including prodigious volumes of documents and files. The next step involves manual validation of customer data that make KYC time-consuming, high-cost, and risk-based operation. On top of it, the continuous need for updating customer data in business logs challenges KYC completion with accuracy and efficiency. There are several challenges to this KYC process of TSPs that can be effectively addressed by AI:

- Absence of centralized KYC database across operators, allowing unregistered telecallers to obtain multiple SIM cards across various operators.
- Absence of AI driven analysis to detect intentional manipulation of KYC documents, specially the photograph to make it look like a different person. This enables the same person to obtain telecom resources exceeding the legally permitted quota.
- Cross-match of KYC documentation for detection of anomalies and patterns thus helping in identification of KYC related frauds. Effective use of anti-counterfeit AI algorithms to detect fraudulent documentation. As

the next step, AI based detection agents / third-parties who are involved in such document / photograph manipulation.

- AI driven automated messages/warnings to end consumers for re-verification and documentation in case of anomaly detection.

II. AI based SPAM detection, enhancement and strict enforcement of Telecom Commercial Communications Customers' Preference Regulations 2018.

The consultation paper rightly highlights that *"The TCCCPR 2018 highlighted that to deal with UCC from Unregistered Tele-Marketers (UTM), signature solutions need to be enhanced which shall be referred to as the UCC Detect System. While determining whether a person or entity is suspected sender of UCC, this system may include additional sources of inputs such as sending information (SI) from reports, inputs collected from Honeypots, information shared by Signature Solutions of other access providers and information available from network elements (examples of which are HLR, and Missed Call Alerts). Such a system would be able to identify suspected UTMs with greater accuracy when it is equipped with more information about suspected UCC senders."*

While the TCCCPR 2018 was a step in the right direction, its half-hearted implementation by TSPs left much to be desired. As a result, SPAM SMS and calls continue in large numbers resulting in significant volumes of financial frauds. With such a huge fraud scenario in place, TSPs in India may be mandated to adopt new innovations that will help combat the rising threat of grey traffic or SMS spamming. One of the emerging technology in this area is AI-powered SMS filters that utilize deep learning artificial intelligence systems to identify and filter spam SMS before they reach the end user. Though one can argue that the DND requests and Spam filtering apps already available on the market can help reduce the onslaught of spam SMS, there isn't a full proof solution to the problem. Besides, there is no way these apps or DND requests would work for vendors who create campaigns and receive spam SMS as a response. Here is where AI enabled filters can make the difference. Most ordinary filters for spam SMS detection targets the source number from which the SMS originated and then look for suspecting URLs in the SMS that redirect readers to fraudulent websites. However, with AI-powered filters, the game changes considerably. There are several algorithms available today that can be trained on AI-powered systems to study textual patterns and determine the proper usage of words and ultimately classify it as legitimate or spam based on the true intent of the message.

Adaptive AI based systems are informed by live data streams from wireless carriers, smartphone devices, and apps. It evaluates every call to look for new patterns that would indicate whether the call is spam, including which carrier originated the call, what country it came from, and if its network signature indicates spam risk. By constantly monitoring these patterns, such system is able to detect spam calls based on shifting tactics instead of relying on phone numbers and historical data. Typical outgoing call patterns are can be analyzed and matched with similar profiles in the same geographic area and numbers with unusually high outgoing to incoming ratios can be flagged for further scrutiny by the ML engine.

TRAI's TCCCPR 2018 Regulations prohibits personal mobile numbers to be used for sending unsolicited commercial messages. AI based detection should be employed to detect text content of SMS messages which can then be used to train ML engines for flagging of such messages from personal numbers.

It is pertinent to point out that several International Carriers have already implemented AI and ML driven models to identify SPAM calls and SMS both in real-time and non-real-time scenarios. UK operator EE, claims it has blocked 11 million scam calls2 since deploying upgraded AI technology to tackle the issue in July 2022 as part of a wider campaign to protect customers. In 2021, almost 45 million people were on the receiving end of potential scam texts or calls in Summer, Ofcom research revealed. More than 82% said they had received a suspicious message, in the form of either a text, recorded message or live phone call to a landline or mobile, this represented an estimated 44.6 million adults in the UK.

The firewall technology from EE uses AI to review calls passing through UK Calling Line Identification (CLI) from other countries and blocks those pretending to be based in the UK, halting scam calls so that they never reach customers.

As well as protecting EE, BT and Plusnet customers, the technology stops inbound calls from international locations using UK numbers from being forwarded to other networks.

[2] https://mobile-magazine.com/technology-and-ai/ee-tackles-spam-calls-and-texts-with-latest-ai-technology

III. AI driven detection of SIM boxes and other illegal hardware

The TCCPR 2018 regulations prohibits any unsolicited commercial communications from 10-digit mobile numbers and restricts such messages only through registered telemarketers who have registered valid Header IDs through any of the available DLT platforms.

However, unscrupulous / unregistered telemarkets often do not register any Header IDs and use personal 10-digit mobile numbers to push high volume of Spam SMS. In order to circumvent the per day limit of 250 SMS, these UTMs make use of SIM boxes, each of which can accommodate hundreds of SIM cards at once and unable RTMs to push thousands of SMS in rapid succession and without any restriction. Clearly, usage of such SIM boxes or similar hardware is a serious contravention of applicable regulations, and must be curbed in order to ensure security of end-consumers.

However, advances in AI and ML technologies have now enables detection of such illegal hardware on real time basis which can be adopted by TSPs, if they are accordingly mandated.

Advanced machine learning (ML) and artificial intelligence (AI) solutions offer powerful end-user configurable platforms to combat simbox fraud, leveraging sophisticated analytics with Explainable AI and automated actions to eliminate sim boxing fraud threats.

These solutions utilize a structured profiling ML model which was be fed with a range of typical usage data, creating a rich dataset as the foundation to rapidly identify events which correlate with suspected simbox usage. The rich dataset may include just a small subset of fraud activities, providing the basis for the system to accurately identify high-risk activities while avoiding any risk of undermining service provision for genuine users.

Similarly, sophisticated machine learning models are able to use fully automated structured profiling analysis of key data points such as number of calls made, SMS sent, duration of calls, number of SMS in a given time, overall usage profile, and other critical parameters to identify different types of activities. This is then coupled with classification modeling to separate fraudulent activity from genuine users. This hybrid ML approach also allows the system to identify evolving anomalous behavior that falls outside the norm, and explain suspicious activity for further investigation or link to new fraud methods. An example is a new type of camouflage calling activity introduced by fraudsters to avoid detection of sim boxing.

Unlike a traditional, static fraud management system, the AI/ML approach provides an adaptive and flexible solution that not only identifies a rigid list of fraud activities, but actively evolves to detect emerging fraud methods and types in real-time.

AI/ML solutions ensure customers' fraud management systems are not only empowered to identify frauds following traditional methods or patterns, but also able to quickly identify emerging anomalous behavior related to new fraud risks. Automated responses can be established to eliminate the threat before financial frauds take place, while high-risk or suspicious cases can be quickly flagged and escalated to analysts for a full review supported by Explainable AI.

3. Conclusion

In view of our aforementioned submissions, we reiterate and summarize our key recommendations as under:

- *AI and ML driven applications may be explored for strengthening and enforcement of existing KYC regulations.*
- *AI based technologies are available for SPAM detection, enhancement and strict enforcement of Telecom Commercial Communications Customers' Preference Regulations 2018. Such technologies may be suitably evaluated for implementation by TSPs.*
- *AI and ML assisted platforms may be deployed by TSPs for the detection of SIM boxes and other illegal hardware.*