BRAND SAFETY

Brand Safety is a key concern on everyone's mind. The industry has been witnessing many stories citing fraud and piracy, untenable ad adjacencies, and debate regarding proper consumer consents to activate targeted services. Thus, we at Scocre addresses many incidents that may cause harm to the brand's name and consumer.

Our Brand Safety document covers a broad range including piracy, malware, fraud, contextual brand safety occurrences, and concerns related to user's privacy and appropriate consent. Scocre values user's safety first, thus, we never ask for user's confidential details without their given consent. We advices our users to be aware of fraudulent calls and pirated activities driven by fraudsters who may trick the users to breach their privacy. Fraudsters may then use the information for illicit activities, violating human rights and personal safety norms.

BRAND SAFETY VIOLATIONS:

We avoid any such content and/or activity that is generally considered inappropriate for promoting the brand. Therefore, anyone using our brand's name for advertising and marketing illicit activities would be considered liable for legal actions.

The Terms and Conditions under the Agreement apply to the performance of services provided by the COMPANY.

A. Scocre Rating Agency and Consulting Private Limited Company and engaged in the business of Consulting Services in the field of Account Origination and Portfolio Management; Credit Information Services, Namely, Providing Credit Information relating to Consumer or Commercial Applicants and for the purpose of credit, utility services such as Credit Evaluation, Analysis and Alert Services and also providing Information relating to Insurance, Credit, Loans and Debt Management. Presently the first party is providing one STOP SOLUTION to get information and best plan to check and review your score electronically via its web portal "SCOCRE" i.e. www.scocre.com.

B. The matters, events, acts as mentioned below shall amount to the violations of Company's Brand Safety norms.

- Click Farms
- Pixel Stuffing
- Ad-Stacking
- Click Injection
- System IP Changer
- Software IP Changer
- Social Media Fraud
- Online Gift Fraud

- Online OTP Bypass
- IP Address
- Proxy
- Location
- System Ip
- Duplicate User
- Fake Traffic
- Data filling
- Duplicate Device

In addition to the above, the stakeholders hereby understand that the following would be considered cyber fraud and would be liable for strict legal actions.

The following including but not limited to:-

1. Subscription which does not seems to be genuine by the Company
2. Package subscribed via duplicate ID, same IP Address
3. Package subscribed via payment of same Banking Details including same debit/credit card
4. Package subscribed via same id of payment apps and/or UPIs
5. Package subscribed consisting of same contact details
6. Subscription which is being made with intention to do any of event as mentioned as above.

Any outsider party shall obtain Company's approval for copy, layouts, artwork, proofs, radio scripts, TV storyboards, scripts and answer prints before executing any advertising idea, plan, program or campaign.