MERCHANT ONBOARDING POLICY

Document name	Merchant Onboarding Policy
Version	v1.2
Document author	Legal & Compliance team
Release date	February 29th, 2024
Last updated on	2nd July, 2025
Review frequency	Annual
Approved by	Board of Directors

TABLE OF CONTENTS

QUICKTOUCH TECHNOLOGIES LIMITED DELHI

1. INTRODUCTION

1.1 The purpose of this Merchant Onboarding Policy ("**Policy**") is to establish a risk-based merchant acceptance policy for merchants seeking to use the payment aggregation services ("**Merchants**") of Quicktouch Technologies Limited ("**Quicktouch**").

1.2 Quicktouch has framed this Policy to lay down the following processes: (a) Merchant risk-identification at the time of onboarding of the Merchant and (b) Merchant assessment throughout the period of the Merchant's association with Quicktouch.

1.3 Quicktouch shall, at all times, undertake these activities in compliance with the applicable laws and relevant rules, regulations and schemes issued by the card payment networks.

2. ONBOARDING RISK PARAMETERS

2.1 For the purpose of onboarding, Quicktouch shall primarily focus on determining and validating the:

a. identity the business carried on by the Merchant in order to determine any associated risk along with its documents and requisites as prescribed by the regulator. ***NOTE: All merchants shall be onboarded strictly in accordance with the internal onboarding checklist as set out in Annexure A.***

2.2 For the purpose of risk assessment, Quicktouch shall collect and verify information from different sources including the following:

a. PAN which shall be verified through the issuing authority or through partnerships with third party service providers.
b. Business KYC documents such as GST certificate, Udyam Aadhaar, Certificate/licence issued by the municipal authorities under Shop and Establishment Act, Utility bills (such as electricity, water, landline telephone bills, etc.), GST and Income Tax returns which shall be verified using third party APIs.
c. Bank account details which shall be verified using penny drop from service provider, including bank statements.
d. Cancelled cheque image which shall be manually verified via the support team.
e. Premises photos, type of business and business location which shall be manually verified by the support team.
f. Terms and conditions, privacy policy and refund policy of the Merchant.
g. Documents required to undertake due diligence of beneficial owners (PAN, Aadhaar, Voter ID, Driving Licence, etc), including qualifications of the directors/promoters and contact details (email and mobile no.) of the authorised signatory.
h. Risk parameters such as credit score, business vintage, domain age, type of business, nature of business, and business turnover shall be collected and checked for validity.

NOTE: If the information provided by the Merchant seems suspicious or fraudulent, the Merchant will be required to justify all the related information and reshare documents when followed up by the support team. Until then, the user shall be blocked from using the Quicktouch's platform.

3. BASIC CHECKS

3.1 Quicktouch shall verify the following details of their Merchants:

i. Location using Google Maps
ii. Name matching on their PAN and Account Information
iii. Automated/manual verification of the business documents
iv. Aadhaar verification for beneficial owners

3.2 Quicktouch shall also check for fraudulent transactions via an internal AML screening tool with rules like transaction throughput and volumes, small value recurrent transactions to the same beneficiary etc. Based on the behaviour identified, risk filtering shall be done for Merchant transactions followed by their manual verification. Merchants shall be whitelisted and thereby would be able to use the app for making transactions.

Moreover, our fraud prevention system incorporates an internal Anti-Money Laundering (AML) screening tool designed to identify suspicious transactions. The system evaluates multiple parameters, including transaction throughput, volume patterns, and recurrent small-value transactions to the same beneficiary. Additionally, after receiving the authorization from the regulator, Quicktouch as a PA shall register with FIU-IND. This will allow us to obtain a Reporting Entity status under PMLA. Further, it will also allow us to flag and report any transactions that meet predefined risk criteria. This layered approach ensures that potential fraudulent activities are detected and mitigated in real time. Quicktouch's internal AML screening tool is designed to detect and prevent fraudulent transactions by implementing advanced rule-based monitoring. These screening tools have a risk-based classification framework, which includes:

- Transaction Limits – Restricting the number of transactions permitted per merchant or customer to mitigate potential risks.
- Suspicious Transaction Blocking – Preventing transactions that exceed predefined risk thresholds from being processed.
- IP, Domain, and Email Blacklisting – Blocking access from IP addresses, domain names, and email IDs linked to fraudulent activities.
- BIN Validation, Card & Mobile Number Restrictions – Identifying and restricting specific card BINs, card numbers, and mobile numbers flagged for suspicious behaviour.
- VPA Monitoring & Blocking – Preventing transactions through Virtual Payment Addresses (VPAs) associated with unauthorized activities.

+91- 96670 09283 Info@quicktouch.co.in 203, D-Mall, Netaji Subhash Place, Pitampura, Delhi - 110034

3.3 Quicktouch shall maintain a list of regions which are blacklisted for Merchant onboarding and any attempt made by agents to onboard from these locations is denied by the system.

3.4 Quicktouch shall regularly update the blacklist regions where onboarding is prohibited through agent-led onboarding. Quicktouch shall use an AML tool to identify any suspicious activity on the transactions of Merchant and block the Merchant. The list is maintained on the basis of regulatory directives, internal risk assessments (high chargeback ratios, suspicious transactions), historical fraud data (merchant fraud, identity theft, money laundering), industry and law enforcement alerts on high-risk locations. The system automatically blocks any onboarding attempt from blacklisted regions, with alerts generated for further review.

Additionally, Quicktouch conducts its own independent verification process to ensure compliance and mitigate risks. All KYC documents submitted undergo a thorough re-evaluation, and enhanced due diligence is performed before finalizing the merchant onboarding. This multilayered approach ensures that only compliant and legitimate merchants are on boarded onto the platform.

3.5 Quicktouch shall also block Merchants based on document verification failure or suspicious transactions. Only after verification of personal and business documents, the user shall be eligible to receive payments. The transaction trails shall also be maintained in the database for reconciliation.

3.6 Information Security:

a. Quicktouch shall strive to work with the Merchants at the time of onboarding to understand how transaction related data is being stored.
b. Quicktouch shall audit where feasible or ask for evidences that customer consent is taken for collecting payments in a secured manner.
c. Quicktouch's agreements mandate the Merchants to use the best practices to secure & store customer and transaction data
d. Quicktouch can instantly block Merchants in case they breach any contractual obligations or are found to be fraudulent

NOTE: The PAs shall obtain periodic security assessment reports either based on the risk assessment (large or small merchants) and / or at the time of renewal of contracts.

Quicktouch mandates that all merchants adhere to best practices for securing and storing customer and transaction data. Quicktouch fully complies with RBI's guidelines regarding the handling of sensitive payment data. Specifically, our system ensures that merchants do not store customer card details, in line with the prescribed regulatory framework. Furthermore, Quicktouch has implemented cards tokenization framework in compliance with RBI guidelines on Tokenization - Card Transactions (RBI/2018-19/103 DPSS.CO.PD No.1463/02.14.003/2018-19_dated January 08, 2019, to ensure tha senstive payment credentials, such as card details, are realaced with secure, system-generated

tokens before processing transactions. Tokenization enhances security by preventing unauthorized access to cardholder data while enabling a seamless and compliant payment experience for merchants and customers.

4. ONBOARDING PROCESS

At QuickPay, we are committed to ensuring a seamless, secure and transparent onboarding experience for our merchants. Our onboarding process is structured to verify the authenticity of merchants, mitigate risk, and ensure full compliance with regulatory standards.

Steps for Merchant Onboarding

I. Merchant Application

- Prospective merchants fill out the online Merchant Application Form (MAF) or sign up directly on our website.
- Required details include business information, category, product/service offerings, and essential documents like GST, PAN, COI, MOA, AOA, financials and registration certificates.

II. KYC & Document Verification

- KYC is mandatory for both the business and its key stakeholders (directors/signatory authority).
- Verification includes:

  ⇒ Company documents (e.g., GST, COI, MOA, AOA, PAN, UDYAM).
  ⇒ Director/Signatory KYC (PAN, Aadhar).
  ⇒ Authorization documents (e.g., board resolution).

III. Background Checks

- QuickPay conducts thorough third-party and manual checks to verify:

  ⇒ Legitimacy of business operations.
  ⇒ Compliance with PCI-DSS, PA-DSS, and tokenization norms.
  ⇒ No involvement in restricted or prohibited business categories.
  ⇒ Website/App compliance with refund/return policies and overall functionality.
  ⇒ Domain and DNS verification

QUICKTOUCH TECHNOLOGIES LIMITED DELHI

+91- 96670 09283 Info@quicktouch.co.in 203, D-Mall, Netaji Subhash Place, Pitampura, Delhi - 110034

IV. **Risk Assessment**

- Evaluation of merchant's business model, operational history, financial stability, and managerial background to assess risk.

V. **Approval & Account Creation**

- Upon successful verification and risk evaluation, the merchant is approved.
- QuickPay registers the merchant on its dashboard and maps appropriate payment modes.
- MDR (Merchant Discount Rate) setup is completed.
- Live credentials are securely shared.

VI. **Compliance Agreement**

- The merchant signs a service agreement that outlines:

  ⇒ Business scope
  ⇒ Data security, privacy, and indemnity obligations.
  ⇒ Settlement cycles and terms of service

VII. After all checks and setups, the merchant account is activated and ready to process transactions on QuickPay's platform.

POST-ONBOARDING: CONTINUOUS MONITORING

QuickPay continues to monitor merchant activities to prevent fraud, ensure policy compliance and support operational transparency. Merchants must report any changes in business structure or key details within 15 days.

5. RESTRICTED MERCHANTS & PROHIBITED MERCHANTS

The level of risk that a Merchant or a prospective client poses shall be identified only upon evaluation of the information provided and additional documents shared by the Merchant. In furtherance of the same, Merchants undertaking the business activities enlisted on the list provided under Schedule I ('Restricted Merchants') would be reviewed with greater scrutiny by Quicktouch. Additionally, Quicktouch shall maintain a list of 'Prohibited Merchants' (under Schedule II) who shall not be qualified to avail services of Quicktouch.

QUICKTOUCH TECHNOLOGIES LIMITED DELHI

+91- 96670 09283 Info@quicktouch.co.in 203, D-Mall, Netaji Subhash Place, Pitampura, Delhi - 110034

ANNEXURE A

LIST OF DOCUMENTS (KYC) FOR ONBOARDING

1. INDIVUDUALS

KYC Document Type	KYC Document Name	KYC Requirement
Proof of Identity	PAN Card	Mandatory
Proof of Address (OVD)	Aadhaar Card	Any One
	Voter ID card	
	Passport	
	Driving License	
	NREGA	
Bank Details	Cancelled Cheque	Mandatory

Where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:

(A) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
(B) property or municipal tax receipt;
(C) pension or family pension payment order issued to retired employees by Government Departments or Public Sector Undertakings, if that contain the address;
(D) letter of allotment of accommodation from employer issued by State Government or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation;

Note - The customer shall submit OVD with current address within a period of three months of submitting the documents specified above.

QUICKTOUCH TECHNOLOGIES LIMITED DELHI

2. SOLE PROPRIETOR

KYC Document Type	KYC Document Name	KYC Requirement
Proof of Identity	PAN Card	Mandatory
	Aadhaar Card	Any One
	Voter ID card	
	Passport	
	Driving License	
Business Legality Proof and Proof of Business Address	a. Registration certificate including Udyam Registration Certificate (URC) issued by the Government	If not registered for GST, take NO GST undertaking and any two of the other documents
	b. Certificate/licence issued by the municipal authorities under Shop and Establishment Act	
	c. Sales and income tax returns	
	d. GST certificate	
	e. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities	
	f. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute	
	g. Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities	
	h. Utility bills such as electricity, water, landline telephone bills, etc which should be not older than 3 months.	
Bank Details	Cancelled Cheque	Mandatory

QUICKTOUCH TECHNOLOGIES LIMITED DELHI

3. PARTNERSHIP FIRM

KYC Document Type	KYC Document Name	KYC Requirement
Proof of Identity(Authorized Signatory)	PAN Card_Authorized Signatory	Mandatory
	Aadhaar Card	Any One
	Voter ID card	
	Passport	
	Driving License	
Business Legality Proof	Partnership Deed with Registration Certificate	Mandatory
	Partnership Authority letter naming Authorised Signatory signed by all Partners / Power of attorney	
	Address of the registered office, and the principal place of its business, if it is different	
	Business PAN Card	
Business Legality Proof and Proof of Business Address	GST certificate	If not registered for GST, take NO GST undertaking and any one of the other two
	Shop & Establishment Certificate issued by a Civic Authority	
	Registration Certificate issued by a Central or State Govt Body e.g. Udyog Aadhaar	
Bank Details	Cancelled Cheque	For Settlement purpose

QUICKTOUCH TECHNOLOGIES LIMITED DELHI

4. PRIVATE LIMITED/ PUBLIC LIMITED

KYC Document Name	KYC Requirement
PAN Card_Authorized Signatory	Mandatory
Aadhaar Card	Any One
Voter ID card	
Passport	
Driving License	
Memorandum and Articles of Association	Mandatory
Certificate of Incorporation	
Address of the registered office, and the principal place of its business, if it is different	
Board Resolution with authorized officials name	
Business PAN Card	
GST certificate	If not registered for GST, take NO GST undertaking and any one of the other two
Shop & Establishment Certificate issued by a Civic Authority	
Registration Certificate issued by a Central or State Govt Body e.g. Udyog Aadhaar	

KYC Document Name
1.Pan Card of Authorised Signatory
2. Proof of Identity of Authorised Signatory
3. Memorandum and Articles of Association
4. Certificate of Incorporation
5. Address of the registered office, and the principal place of its business, if it is different
6. Board Resolution with authorized officials name
7. Business PAN Card
8. GST certificate
9. Shop & Establishment Certificate issued by a Civic Authority
10.Registration Certificate issued by a Central or State Govt Body e.g. Udyog Aadhaar
11. Cancelled cheque for settlement purpose

QUICKTOUCH TECHNOLOGIES LIMITED DELHI

5. LLP

KYC Document Type	KYC Document Name	KYC Requirement
Proof of Identity(Authorized Signatory)	PAN Card_Authorized Signatory	Mandatory
	Aadhaar Card	Any One
	Voter ID card	
	Passport	
	Driving License	
Business Legality Proof	LLP agreement / Deed /Limited Liability Partnerships	Mandatory
	Address of the registered office, and the principal place of its business, if it is different	
	Business PAN Card	
	Certification of Incorporation/Registration certificate	
Business Legality Proof and Proof of Business Address	GST certificate	If not registered for GST, take NO GST undertaking and any one of the other two
	Shop & Establishment Certificate issued by a Civic Authority	
	Registration Certificate issued by a Central or State Govt Body e.g. Udyog Aadhaar	
Bank Details	Cancelled Cheque	Mandatory

QUICKTOUCH TECHNOLOGIES LIMITED DELHI

6. SOCIETIES & TRUST

KYC Document Name	KYC Requirement
PAN Card	Mandatory
Aadhaar Card	Any One
Voter ID card	
Passport	
Driving License	
Registration Certificate of Society/Trust deed	Mandatory
Business PAN Card	Mandatory
Authority letter for authorized signatory by members	Optional
Society Bye-laws	Mandatory
Latest maintenance bill in the name of applicant for a period of 3 Months	Any One
Latest copy of electricity bill in the name of applicant for a period of 3 Months	
Latest copy of Landline bill in the name of applicant for a period of 3 months	

Required Documents		
1	Bank - Proof	Cancelled Cheque / bank Statement
2	POI - Entity	Pan Card Society / Trust
3	POA - Entity	Trust GST Certificate / Society Registration Certificate
4	Business Constitution Proof	Society / Trust Registration Deed
5	POA - Authorized signatory	Pan Card + Aadhar Card
6	Affiliation Certificate	Need Affiliation certificate/ no. for School if available
7	Authorization proof	Declaration by trust/ society for Authorized signatory

QUICKTOUCH TECHNOLOGIES LIMITED DELHI

QUICK TOUCH
INNOVATING INTERESTINGLY

MERCHANT ONBOARDING OPERATIONAL AND DUE DILIGENCE CHECKLIST

Category	Checklist Points
1. KYC & Business Verification	• Valid business registration (GST, COI, Shop Act, etc.) • PAN, Aadhaar, signatory ID • Address proof & live photo/selfie • Bank account verification
2. Website / Digital Presence Check	• Active website with valid domain • SSL certificate (HTTPS) • Web crawling for T&C, privacy, refund policy, contact info • No redirections or harmful content • Verified social media handles
3. Operational Risk Assessment	• Business model allowed as per policy • No prohibited category (gambling, crypto, etc.) • Fulfilment & delivery verification • Physical/virtual site check (as applicable) • Merchant operations questionnaire
4. Financial Review	• Bank statement (3–6 months) • Expected transaction volume and average ticket size • Previous processor/credit reference (if applicable)
5. Legal & Compliance Checks	• Sanctions/Watchlist/PEP screening • Director background checks • UBO identification & verification • Merchant agreement signed • Information security & compliance declaration
6. Technology & Security Review	• PCI-DSS compliance (if applicable) • Secure API/plugin integration • Use of tokenization/vaulting • Secure hosting & infrastructure • Role-based access and fraud detection in place
7. Ongoing Monitoring & Risk Flags	• Chargeback/refund tracking • Sudden spike alerting • Periodic re-KYC & risk reviews • Blacklist/greylist watchlist • Automated website crawling at intervals

QUICKTOUCH TECHNOLOGIES LIMITED DELHI

QUICK TOUCH
INNOVATING INTERESTINGLY

FOR WEBSITE

Factors to Review a Website for Compliance and Verification:

1. **Privacy Policy:** Ensure a clear and comprehensive policy for data collection, usage, storage, and sharing is displayed.
2. **Terms of Use/ Terms & Conditions:** Provide detailed user agreements, including permissible use, disclaimers, and liability clauses.
3. **Content Authenticity:** Verify the accuracy and ownership of educational materials to avoid copyright issues.
4. **Age-Appropriate Content:** Ensure content is suitable for the intended audience and complies regulations for minors.
5. **Dispute Resolution/ Grievance Policy:** Outline clear procedures for handling grievances and disputes.
6. **License and Accreditation:** Display necessary certifications, licenses or affiliations with educational bodies.
7. **Web Crawling:** Use automated tools or manual checks to scan
8. **Web Scraping Alerts:** Cross-reference domain content with known blacklists, adult, illegal, or scam sites
9. **Refund Policy**
10. **Cancellation Policy**
11. **About Us**
12. **Contact Us Page**
13. **Check if all Tabs are working**
14. **Share test credentials/ demo credentials if possible.**

QUICKTOUCH TECHNOLOGIES LIMITED DELHI

+91- 96670 09283
Info@quicktouch.co.in
203, D-Mall, Netaji Subhash Place, Pitampura, Delhi - 110034

QUICK TOUCH
INNOVATING INTERESTINGLY

Merchant Information Security Review Checklist

#	Checklist Item	Yes / No	Remarks
1	Merchant has a valid business registration and KYC documentation.		
2	Merchant website/domain is active and securely hosted (HTTPS).		
3	SSL certificate is valid and up to date.		
4	Merchant has implemented secure login and user authentication for internal systems.		
5	PCI-DSS compliance certificate (if applicable) is available and valid.		
6	Data encryption is used for storing and transmitting sensitive information.		
7	Merchant confirms non-storage of CVV, PIN, or full card numbers (as per RBI/PCI rules).		
8	Adequate access control and role-based access to customer/transaction data.		
9	Merchant has defined an internal data privacy policy.		
10	Incident Response Plan is in place for handling data breaches or fraud.		
11	Regular vulnerability scans and penetration testing are conducted.		
12	Merchant maintains logs of all transactions and access for audit purposes.		
13	Anti-malware and anti-virus protections are deployed and regularly updated.		
14	Web application firewall (WAF) or similar tools are in use.		
15	Secure coding practices are followed for proprietary applications.		
16	Merchant infrastructure (servers, networks) is adequately secured.		
17	Two-factor authentication (2FA) is enabled for admin access.		
18	Secure payment gateway integration is verified (API or hosted page).		
19	Merchant uses tokenization or similar techniques to protect payment data.		
20	Merchant agrees to comply with applicable data protection laws (e.g., IT Act, GDPR, DPDP).		
21	History of past security incidents or fraud reported (if any).		
22	Terms of Use and Privacy Policy are publicly displayed and accessible.		
23	Refund and dispute resolution process is clearly defined and followed.		
24	Merchant agrees to periodic compliance audits by the Payment Aggregator.		
25	Merchant signs the Information Security Compliance Declaration.		

QUICKTOUCH TECHNOLOGIES LIMITED DELHI

+91- 96670 09283
Info@quicktouch.co.in
203, D-Mall, Netaji Subhash Place, Pitampura, Delhi - 110034

SCHEDULE I
RESTRICTED MERCHANTS

1. Cable descramblers and black boxes which includes devices intended to obtain cable and satellite signals for free;
2. Bulk marketing tools which include email lists, software, or other products enabling unsolicited email messages (spam);
3. Mining / oil drilling & refining;
4. Houses of worship (e.g., churches, temples etc. for donations) / fund raising by political, religious organizations or institutions / charities or non-profit organizations;
5. Merchants engaged in products or services where specific licenses are required to operate in local jurisdiction;
6. Merchant establishments where the promoter/partner/proprietor/owner's name appear in the RBI defaulters/negative list/bank's internal negative list or such other list which may be published by the bank from time to time;
7. Credit repair or protection or restoration;
8. Dating/Matrimonial services;
9. Charities/Donations;
10. Auction houses;
11. Real Estate agents/brokers;
12. Prepaid cards;
13. Shall create liability for us or cause us to lose (in whole or part) the services of our Internet Service Provider ("ISPs") or other suppliers.
14. Web Hosting;
15. Resume writing and Recruitment services
16. Remote Access Technical Support;
17. Matrix sites or sites using a matrix scheme approach;
18. Work-at-home information;
19. Drop-shipped merchandise;
20. Regulated goods which includes air bags, batteries containing mercury, Freon or similar substances/refrigerants, chemical/industrial solvents, government uniforms, car titles, license plates, police badges and law enforcement equipment, lock-picking devices, pesticides, postage meters, recalled items, slot machines, surveillance equipment, goods regulated by government or other agency specifications;
21. Securities which includes stocks, bonds, or related financial products;
22. Prescription drugs or herbal drugs or any kind of online pharmacies which includes drugs or other products requiring a prescription by a licensed medical practitioner;
23. Gaming/gambling which includes lottery tickets, sports bets, memberships/ enrolment in online gambling sites, and related content.

QUICKTOUCH TECHNOLOGIES LIMITED DELHI

+91- 96670 09283
Info@quicktouch.co.in
203, D-Mall, Netaji Subhash Place, Pitampura, Delhi - 110034

SCHEDULE II
PROHIBITED MERCHANTS

1. Adult goods and services which includes pornography and other sexually suggestive materials (including literature, imagery and other media, escort or prostitution services);
2. Alcohol or goods which includes Alcohol content or any other alcoholic beverages such as beer, liquor, wine, or champagne;
3. Body parts which includes organs or other body parts including blood and other bodily fluids - live, cultured/preserved or from cadaver;
4. Child pornography which includes pornographic materials involving minors;
5. Copyright unlocking devices which includes Mod chips or other devices designed to circumvent copyright protection;
6. Copyrighted media which includes unauthorized copies of books, music, movies, and other licensed or protected materials;
7. Copyrighted software which includes unauthorized copies of software, video games and other licensed or protected materials, including OEM or bundled software;
8. Counterfeit and unauthorized goods which includes replicas or imitations of designer goods; items without a celebrity endorsement that would normally require such an association; fake autographs, counterfeit stamps, and other potentially unauthorized goods;
9. Drugs and drug paraphernalia which includes illegal drugs and drug accessories, including herbal drugs like salvia and magic mushrooms;
10. Drug test circumvention aids which includes drug cleansing shakes, urine test additives, and related items;
11. Endangered species which includes plants, animals or other organisms (including product derivatives) in danger of extinction;
12. Government IDs or documents which includes fake IDs, passports, diplomas, and noble titles;
13. Hacking and cracking materials which includes manuals, how-to guides, information, or equipment enabling illegal access to software, servers, websites, or other protected property;
14. Illegal goods which includes materials, products, or information promoting illegal goods or enabling illegal acts;
15. Miracle cures which includes unsubstantiated cures, remedies or other items marketed as quick health fixes;
16. Offensive goods which includes literature, products or other materials that: a) Defame or slander any person or groups of people based on race, ethnicity, national origin, religion, sex, or other factors b) Encourage or incite violent acts c) Promote intolerance or hatred;
17. Offensive goods, crime scene photos or items, such as personal belongings, associated with criminals;
18. Pyrotechnic devices and hazardous materials which includes fireworks and related goods; toxic, flammable, and radioactive materials and substances;
19. Tobacco and cigarettes which includes cigarettes, cigars, chewing tobacco, electronic cigarettes and related products;

QUICKTOUCH TECHNOLOGIES LIMITED DELHI

+91- 96670 09283
Info@quicktouch.co.in
203, D-Mall, Netaji Subhash Place, Pitampura, Delhi - 110034

20. Traffic devices which includes radar detectors/jammers, license plate covers, traffic signal changers, and related products;
21. Weapons which includes firearms, ammunition, knives, brass knuckles, gun parts, military arms and other armaments;
22. Wholesale currency which includes discounted currencies or currency exchanges;
23. Live animals or hides/skins/teeth, nails and other parts etc. of animals;
24. Multi-Level Marketing collection fees;
25. Overseas foreign exchange trading;
26. Any product or service which is not in compliance with all applicable laws and regulations whether federal, state, local or international including the laws of US;
27. Illegal weapons, Product violating someone's privacy, providing or creating computer viruses;
28. Product that tries to gain unauthorized access or exceeds the scope of authorized access to the website, profiles, blogs, communities, account information, bulletins, friend requests, or other areas of the website, or solicits passwords or personal identifying information for commercial or unlawful purposes from other users on the website;
29. Interferes with another's use and enjoyment of the website;
30. Threatens the unity, integrity, defense, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any offence or prevents investigation of any offence or is insulting any other nation;
31. Shall, directly or indirectly, offer or attempt to offer trade or attempt to trade in any item which is prohibited or restricted in any manner under the provisions of any applicable law, rule, regulation or guideline for the time being in force;
32. Fortune tellers/Astrology;
33. Adoption of children and babies;
34. Code that carries out any "denial of service" or any other harmful attacks on application or internet service;
35. Inappropriate, illegal or otherwise prohibited communication to any newsgroup, mailing list, chat facility, or other internet forum;
36. Disruption, placing unreasonable burdens or excessive loads on, interfere with or attempt to make or attempt any unauthorized access to the store of any other user;
37. Antisocial, disruptive, or destructive acts, including "flaming," "spamming," "flooding," "trolling," and "briefing" as those terms are commonly understood and used on the internet;
38. Block chain and digital payment systems such as Bitcoins.
39. Betting, bookmaking, racing – car/ animals;
40. Political candidates or political organizations;
41. Pornography goods/stores, companion / escort services, dating services/ matchmaker services, online adult membership, adult book stores, adult telephone conversations;
42. Lobby groups;
43. Entities engaged in chit funds / unauthorized financial schemes;
44. Entities owned by politically exposed persons (promoters/owners);
45. International Merchants not having local presence in India.

QUICKTOUCH TECHNOLOGIES LIMITED DELHI

+91- 96670 09283 Info@quicktouch.co.in 203, D-Mall, Netaji Subhash Place, Pitampura, Delhi - 110034