digio

Merchant Onboarding Policy

Version No: 3.0

Document Information:

Date of Release	10-Mar-2024
Document Author	Legal and Compliance Department
Document Owner	Legal and Compliance Department
Document Reviewer	Rishabh Upman, Head of Customer Success
Document Approver	Board of Directors
Document Classification	Public

Version History:

Version Number	Authored By	Approved By	Approved On	Description of Change
1.0	Legal and Compliance Department	Board of Directors	15-Mar-2022	Initial Version
2.0	Legal and Compliance Department	Board of Directors	15-Mar-2023	Reviewed and no change
3.0	Legal and Compliance Department	Board of Directors	10-Mar-2024	- Additional KYC and Due Diligence, Infosec Checks - Tasks performed by KYC Officer/ Nodal Officer

digio

Table of Contents

SL No.	Contents	Page No.
1.	INTRODUCTION	03
2.	BASIC CHECKS	03
3.	ONBOARDING PROCESS	05
4.	RESTRICTED MERCHANTED	07
5.	ENHANCED DUE DILIGENCE FOR RESTRICTED MERCHANTS	08
6.	PROHIBITED MERCHANTS	08
7.	DATA PRIVACY	08
8.	COMPLIANCE	08
9.	REVIEW	09
10.	QUALITY REVIEW	09
11.	REVIEW OF EXCEPTIONS GRANTED UNDER THE POLICY	09
12.	SCHEDULE I – DESIGNATED OFFICERS	10
13.	SCHEDULE II – RESTRICTED MERCHANTS	11
14.	SCHEDULE III – PROHIBITED MERCHANTS	13

digio

1. INTRODUCTION

- The purpose of this Merchant Onboarding Policy ("**Policy**") is to establish a risk-based Merchant acceptance policy for Merchants seeking to use Digio's payment aggregation services.
- Digio 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 time of Merchant's association with Digio. Digio, 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.
- Digio provides payment aggregation services to many players in the BFSI industry ("**Merchants**") in order to enable them to accept payments from their customers.

2. BASIC CHECKS

In order to authenticate the identity of the Merchant and any associated risks, Digio undertakes the following checks during the merchant onboarding process:

- Digio, as a policy practice, provides this service offering to only Merchants of high repute. This is evaluated by undertaking a thorough market research, including review of information from the Merchant's website, internet platforms, Facebook, Twitter, LinkedIn or other social media handles and consumer blogs. Digio undertakes a background check and antecedent check of Merchants in a commercially reasonable way, to ensure that Merchants do not have any malafide intention of duping customers, do not sell fake / counterfeit / prohibited products, etc.
- Digio evaluates the nature of the business of the Merchant and whether such business is explicitly allowed under Indian law and any other potential regulatory governance which might be associated with the business. Digio evaluates the transaction volumes being undertaken by the Merchant, the type of entity (LLP, sole proprietor, Partnership, Trust, Individual, Private Limited/Public Limited Company), verifies the location of the business of the Merchant to be in India, and the type of services being sold by the Merchant.

- Verification of the Merchant: For such a purpose, Digio requires the Merchant to submit the following documents, as applicable by entity type: Certificate of Incorporation, GSTIN, PAN, AoA, MoA, Udyam Aadhaar, License (if regulated), Affiliation certificate (if affiliated), Shareholding pattern, UBO/SBO details, List of Directors, Registered deed (for society/trust/partnership) of the Merchant and any other suitable evidence that verifies for authenticity of the organization and status.
- KYC documentation of Promoters/Directors/Authorized signatories (as applicable) for establishing the identity of the operators and verifying the same for authenticity and a copy of the board resolution authorizing the authorized signatory to act on the Merchant's behalf.
- Canceled cheque or Current Bank account statement, with penny drop for bank account verification. In certain cases, Digio also reserves the right to seek a Banker's letter for an account in good standing.
- Matching and tallying Merchant organization's KYC documents and Bank account beneficiary details.
- Screening the Merchants (a) for Politically exposed persons; (b) for compliance with anti-money laundering laws and (c) against the following sanctions lists:
  - OFAC official website - https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information
  - Sanction Screening https://sanctionssearch.ofac.treas.gov/
  - ISIL (Da'esh) & Al-Qaida Sanctions List: https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list
  - The "1988 Sanctions List", consisting of individuals and entities associated with the Taliban which is available at: https://www.un.org/securitycouncil/sanctions/1988/materials.
  - Blacklisted organizations as published by RBI from time to time
  - Any other sanction list that Digio would be required to examine in order to comply with the applicable laws.
- Digio KYC officer also conducts a V-CIP of the Merchant Director/Promoter/Authorized Signatory as well as a Video PD based out the principal business premises of the Merchant as part of additional checks

digio

- Digio performs its Merchant KYC in accordance with the Master Directions for KYC published by the RBI from time to time available here: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11566&Mode=0
- As a continued evaluation mechanism, Digio monitors the transaction logs of the Merchant and investigates in case any unusual activity is noted. The concerned team interacts with the Merchant to understand further and take appropriate action as applicable.

3. ONBOARDING PROCESS

3.1 Timeframes

Typical onboarding process takes 3 to 7 working days. The review process commences with collection of the list of documents mentioned under section 2 of the Policy. Any notice regarding any additional information, documents required is made by the Sales Manager within 2 working days. The Merchants are simultaneously required to fill out an onboarding checklist while Digio's Internal Risk Team scrutinizes the documents submitted by the Merchant. Upon receiving a go-ahead from the Internal Risk Team, Digio signs a master services agreement with the Merchant. The agreement clearly lists down the Merchant's obligations, including clear adherence to all applicable laws at all times during the Merchant's association with Digio. In addition to the above-mentioned agreement, Digio also, as a matter of policy, enters into a non-disclosure agreement with the Merchant.

3.2 Designated Officers

The onboarding activities are typically undertaken by Digio's Internal Risk Team, the Compliance Officer / KYC officer / Nodal Officer and the Sales Manager. While the Sales Team's responsibility is restricted to collating the requisite KYC documents, the Internal Risk Team and the Compliance Officer are responsible for reviewing the documents so submitted and granting approval for onboarding (further details of which are provided under Schedule I of the Policy). The processes undertaken are as follows:

- Collection of requisite KYC documents from the Merchant by the Sales Manager (alternatively, the Merchant can submit the same via the self-upload option provided to the Merchant).
- Verification of the KYC and other requisite documents by the Internal Risk team and the Compliance Officer / KYC officer / Nodal Officer
- Whitelisting of Merchant bank account furnished post verification of bank account. Digio shall perform the same via. doing a penny drop/ penny less transaction
- Tallying of bank account beneficiary and merchant KYC documentation.
- KYC and beneficiary account addition completion confirmation, provided to the Merchant.
- Signing of the master services agreement (MSA) and the Non-disclosure Agreement (NDA) by the Merchant post KYC completion of the KYC verification Process.
- Once the MSA and NDA are signed, the onboarding process is completed.

3.3 Escalated Approval Requirements

The Internal Risk Team and the Compliance Officer shall determine the circumstances under which a Merchant shall be subject to escalated approval requirements on a case-to-case basis, depending on the nature of services availed and the level of risk involved. Any approval granted on an escalated approval basis shall be adequately documented.

3.4 Documentation

Digio follows a thorough documentation procedure with respect to the KYC verification process for each Merchant and the consequent approvals/rejections granted, along with the reasons for such approval or rejection.

Further, Digio's website shall clearly indicate the terms and conditions of the service and time-line for processing chargebacks, returns and refunds, if applicable.

3.5 Alteration

Digio follows a standard process for updating any of the details of any of the Merchants. Any amendment of

digio

information post onboarding shall be executed in accordance with the regulatory requirements. The Merchant will be required to submit relevant proof of change. As a general protocol the following measures are undertaken by Digio:

- In case there is a change in the ownership, Digio undertakes the KYC verification of the new owner based on the protocol mentioned above.
- In the event there is a change in the legal name, Digio shall, in addition to undertaking fresh KYC verification, would check if the change in the legal name results in any change in the type of the business entity.
- If there is a change in the bank account, Digio would withhold the settlement of payments to the Merchant until the account details of the new bank account are verified in accordance with the verification procedures listed above.

3.6 Maintenance of records

All Merchant records and documentation, including documentation in support of the approval for onboarding of the Merchant, are stored digitally in the internal drives dedicated for Digio. The details will be retained perennially.

3.7 Compliance Officer

The Co-founder/ Chief Operating Officer performs this role presently. The Compliance Officer/Nodal Officer ensures adequate compliance with the provisions of the Policy.

4. RESTRICTED MERCHANTS

The level of risk that a Merchant or a prospective client pose is 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 II ("**Restricted Merchants**") would be reviewed with greater scrutiny by Digio.

digio

5. ENHANCED DUE DILIGENCE FOR RESTRICTED MERCHANTS

Upon assessment, if any client is identified as a Restricted Merchant, or upon the discretion and decision of the Digio staff conducting the KYC, additional evaluation will be carried out and the Merchant will be required to complete a risk assessment checklist and simultaneously Digio will identify mitigating factors for the risks posed. In the event Digio concludes that the risks cannot be mitigated, the onboarding will not be processed further. Additional due diligence includes, but is not limited to:

- Seeking and understanding the Audited Financial statements and Income Tax Returns of the Merchant
- Delving deeper into documentation of Ultimate beneficial ownership or Significant Beneficial ownership of the entity
- Conducting interview/PD with the Merchant's Director/Promoter/Authorized Signatory

6. PROHIBITED MERCHANTS

Digio recognizes that certain categories of Merchants carry more risk than others. In furtherance of this and similar lists maintained by Digio's partner banks, payment processors and payment schemes, the categories of Merchants listed in Schedule III shall be considered to fall under the category of '**Prohibited Merchants**' by Digio and shall not be qualified to avail the services of Digio.

7. DATA PRIVACY

Digio shall handle all Merchant-related data in accordance with the Applicable Laws. The Privacy Policy has been published on Digio's website at Privacy Policy.

8. COMPLIANCE

- Digio would undertake a comprehensive security assessment during the merchant onboarding process and ensure merchants adhere to prescribed guidelines as per Applicable Laws. Digio collects Information Security Assessment Audit reports including but not limited to, Appsec, VAPT, Cybersecurity audits, ISO Audit report/certification details for large Merchants who are integrating with Digio APIs

digio

- Digio has published all merchant related policies including but not limited to the terms and conditions on the website.

9. REVIEW

The client account management team along with the Internal Risk Team at Digio carries out a periodic review of Merchant documents. Additionally, an annual audit of the client accounts along with Merchant documents is conducted as part of the statutory audit process.

10. QUALITY REVIEW

Digio looks at the volume of transactions, use case review, intent for expansion of use cases (if any), mandate registration success/ failure percentage, key concerns, mandate presentation success/ failure percentage, failure reasons, recommendations pertaining to the same. This activity is conducted once every 60-90 days.

11. REVIEW OF EXCEPTIONS GRANTED UNDER THIS POLICY

The onboarding policy is followed across all services and for all Merchants and any deviation from the same shall be strictly followed only with the approval of the senior management and is well documented for.

digio

SCHEDULE I

DESIGNATED OFFICERS

Designation	Role
Sales Manager	Responsible for interacting with the client and internal legal team to complete the customer onboarding process including KYC checks, agreement execution, etc
KYC Officer / Nodal Officer	KYC checks, Due Diligence
Head of Business	Reviews commercial terms, nature of services.
Co-founder	Authorized signatory to approve the Master Service Agreement between Digio and the Merchant and execute agreements.

digio

SCHEDULE II

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 includes 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. Money changers, remittance services, money transmitters, check cashing business, currency exchange; and/or
6. Merchants engaged in products or services where specific licenses are required to operate in local jurisdiction;
7. 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;
8. Companies engaged in financial services which are not regulated by RBI/any other regulatory body or where relevant licenses are not available even though required;
9. Credit repair or protection or restoration;
10. Dating/Matrimonial services;
11. Charities/Donations;
12. Auction houses;
13. Real Estate agents/brokers;
14. Prepaid cards;
15. 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.
16. Web Hosting;
17. Resume writing and Recruitment services
18. Remote Access Technical Support;
19. Matrix sites or sites using a matrix scheme approach;
20. Work-at-home information;
21. Drop-shipped merchandise;
22. 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;

23. Securities which includes stocks, bonds, or related financial products;
24. 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;
25. Gaming/gambling which includes lottery tickets, sports bets, memberships/ enrolment in online gambling sites, and related content;

digio

SCHEDULE III

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;
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 (as defined in GMAS Terms) 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;
46. Merchants blacklisted by associations (NMAS/MATCH database).