SBICAP Securities Limited

Marathon Futurex, 12th Floor, B –Wing,

N M Joshi Marg, Lower Parel, Mumbai 400013

REQUEST FOR PROPOSAL
For
Revamp of CRM: Customer Relationship Management

Sr. No	Activity	Details
1	RFP Number	SSL/RFP-014/2022-23
2	Bid Document availability including changes/amendments, if any to be issued	RFP may be downloaded from Company's website https://www.sbisecurities.in/procurement-news
3	Release of RFP	21-March-2023
4	Pre Bid	Queries on email
4	Technical & Commercial Bid submission	12-April-2023
5	Technical Bid Opening	17-April-2023
6	Technical Bid Evaluation and Presentation of shortlisted Service Providers	19-April-2023
7	Opening of Commercial Bids	24-April-2023
8	Method of Selection	Techno commercials (Tech-70%, Commercial-30%)
9	Reverse Auction	28-April-2023
10	Bid Submission Contact Details	**Ms. Trushita Tarkar/Mr. Paren Shah (IT- Department),SBICAP Securities Limited Marathon Futurex, 12th Floor, B Wing, N. M. Joshi Marg, Lower Parel, Mumbai – 400 013. Maharashtra, India. Email ID: Trushita.tarkar@ sbicapsec.com SSLIT-Procurement@sbicapsec.com**

Contents

Introduction:

SSL is a 100% subsidiary of SBI Capital Markets Ltd. which is one of the oldest players in the Indian Capital Market and has a dominant position in the Indian primary capital markets. SBI Capital Markets Ltd. commenced broking activities in March 2001 to fulfil the secondary market needs of Financial Institutions, FIIs, Mutual Funds, Corporate, High Net worth Individuals, Non-resident Investors and Domestic Retail investors. SSL commenced its stock broking operations as a separate Company in the year 2006. The Company is today, a reputed player in the market and has plans to grow its market share to reach the position of one of the largest players in its business. SSL is registered with the Securities Exchange Board of India for its various services, a summary of which is as under:-

SBICAP Securities Limited, hereafter called SSL and Request for Proposal hereafter called RFP.

Registered with/as	Registration no.
SEBI - Stock Broker-NSE	INB231052938
SEBI- Stock Broker-BSE	INB011053031
SEBI- Stock Broker-NSE(F&O)	INF231052938
SEBI- Depository Participant	IN-DP-CDSL-370-2006
SEBI – Portfolio Manager	INP000002098

1. **Request for Proposal (RFP) & Objective**

   This request for proposal document ('RFP document' or 'RFP') has been prepared solely for the purpose of enabling SSL to select a Bidder for supply, implementation, data migration and support of a Customer Relationship Management (CRM) solution through the tenure of the contract.

2. **Scope of work**

   SSL prefers to have a CRM Platform which provides an Omni Channel experience in standard CRM Modules like Customer Management, Lead Management, Service Management and Campaign Management across all branches and departments on an integrated platform along with reporting. The solution stack shall comprise of best of the breed solutions to meet and exceed the business requirements. Also, the Platform be capable of adding integrated modules with built-in workflows, reporting, dashboards etc. Solution shall also be accessible with low bandwidth consumption across all branches of SSL.

   One of the key focus areas is to move towards a customer centric model, wherein the key strategic themes would be towards increasing a customer's lifetime value, reducing cost to serve and designing strategy and decision-making models based on analytical models.

   With the implementation of the new CRM platform, the expectation is to pave the way to a world class, digitized sales journey, marketing and a seamless and hyper personalized customer experience along with customer service with targeted value delivery across channels for SSL.

3. **Eligibility Criteria**

   Only those Bidders who fulfil the following criteria are eligible to respond to the RFP. Document/s in support of eligibility criteria are required to be submitted along with the Technical Bid. Offers received from the bidders who do not fulfil any of the following eligibility criteria are liable to be rejected.

- The bidder should be a company registered in India as per Company Act 1956 /2013 or a partnership firm / a Limited Liability Partnership company under the Limited Liability Partnership Act 2008 in India for last 3 years from the date of RFP. (Certificate of incorporation/Registration is to be submitted) and the support facility within Mumbai will be preferred.

- Bidder should have minimum annual turnover of Rs.50 Crore per annum from software development & implementation each during last three financial years (2019-2020, 2020-21, 2021-22). This must be the individual company turnover and not that of any group of companies. (Copies of the audited balance sheet and P&L Statement of the company showing the same is to be submitted).

- The bidder should have positive operating Profit (as EBITDA i.e. Earnings, Before Interest, Tax, Depreciation & Amortization) in the last three financial years, (2019-20, 2020-21, 2021-22). (Copies of the audited balance sheet and Profit/Loss statement of the firm is to be submitted.)

- The bidder should be the Authorized Partner / Reseller of the Proposed Solution on the date of RFP, with an authority to sell, upgrade, supply, service and maintain the proposed Solution.

- The bidder must submit a letter from the OEM confirming the "Back-to-Back" agreement / arrangement for next 5 years of continuous service /support to SSL, if the contract is awarded to the bidder.

The Bidder should be OEM/OSD for Proposed Solution or their authorized channel partners or Service Provider (SP) or System Integrator (SI) in India with an authority to do customization/up-gradation during the period of contract. Bidder needs to provide Manufacturer Authorization Form (MAF) from OEM stating that bidder is authorized partner of OEM and authorized to participate in this tender and in case the bidder is not able to perform obligations as per contract during the contract period, contracted services will be provided by OEM within the stipulated time. Either OEM/OSD or their authorized partner should participate in the RFP. In case, both OEM & his authorized partner participate, only bid of the OEM/OSD will be considered. Only bidder with one solution / OEM is allowed to bid. Bidders submitting multiple bids of different platforms will be disqualified.

- The bidder must have own/Rented/Registered support offices in India.(Address and Contact details should be submitted)

- Bidder/OEM must have supplied & implemented the Proposed Solution in BFSI companies – (BFSI - Banking Financial Services and Insurance) during the past 3 years in India. Implementation with a broking company will have an added advantage (The bidder has to submit Purchase Order/Satisfactory Certificate from the organization as supporting documents for the same.)

- The companies or firms, bidding for the above tender, should have not been black listed by any of Government Authority or Public Sector Undertaking (PSUs). The bidder shall give an undertaking (on their letter head) that they have not been black listed by any of the Govt. Authority or PSUs. In case, in the past, the name of their Company was black listed by any of the Govt. Authority or PSUs, the same must have been removed from the black list as on date of submission of the tender, otherwise the bid will not be considered.

- The bidder should have a team of at least 50 people to support product development, implementation, and support for CRM solution on their roles along with minimum 25 people being certified on the platform or solution being proposed. The sub-contracting of the implementation / customisation to a 3rd party is not allowed.

> If the bidder is proposing a cloud-based CRM solution (SAAS or infra on cloud) then all CRM data should be stored in India Datacentre for both Primary & Disaster Recovery site

> Proposed CRM should be listed in Gartner Magic Quadrant for the CRM Customer Engagement Centre, Lead management & marketing.

> Queries regarding RFP should be raised at least 5 working days prior to the RFP closure date.

Note: Vendor must comply with the above-mentioned criteria. Non-compliance to any of the criteria can lead to rejection of the offer. Photocopies of relevant documents/certificates should be submitted as proof in support of the claims made for each of the above-mentioned criteria. SSL reserves the right to verify/evaluate the claims made by the vendor independently. Any misrepresentation will entail rejection of the offer.

4. **Broad Scope of Work**

1. All the features in SSL's current CRM Application has to be included in the proposed solution. Vendor team shall ensure all existing features in the new solution. Standard Modules which shall be present in the solution are:
   - Customer 360
   - Customer dashboards
   - Reports & analytics
   - Admin module – Role based permissions
   - Lead Management
   - Ticket management system
   - Telephonic integration
   - Customer voice
   - Alerts and trigger management
   - Engagement tool (Emails, SMS, WhatsApp, etc)
   - Reputation experience management
   - Live chat & chatbot
   - Customer query, request & complaint management
   - Automated workflow
   - Knowledge management
   - Campaign Management
   - Workflow Management
   - Omni Channel Support
   - Agents' presence information
   - Defining agents' capacity
   - Message templates
   - Monitor real-time customer satisfaction
   - Agent Modules - (scripts, Assists, Dashboard, Collaboration)
   - File attachment capability
   - Conversation transcripts

- Social messaging channel
- System shall facilitate easy integration by either providing API or capability to consume APIs.
- Reporting and Dashboard with Drilldown
- Conversation insights
- Customer service insights
- Forecast management
- Sales sequence model
- Contact management & business card scanner
- Opportunity management
- Goal management
- Social Media Integration (Facebook, Whatsapp, Instagram etc.).
- ETL Module for Data Integration
- Custom Web Portal (For Lead, Customer Service & Campaign Activity).

In addition to the above modules, all other standard modules/functionalities available in the market presently suited to BFSI companies – (BFSI - Banking Financial Services and Insurance) sector (Broking, Third party products & Retail lending preferred) shall be proposed in the solution along with case studies, functional specification documents and other documents relevant for showcasing the same.

2. The hardware, software specification, Server Side, Client Side and Network Bandwidth required for the proposed CRM solution needs to be shared by the bidder in the response. Bidder also need to share Deployment Model, Software Architecture diagram, Network Architecture Diagram, Schema Design, Performance Benchmark of the solution, Benchmark of Data Import process of the solution, Product Specifications (Functionality Specification Documents, Brochures, Videos' etc), User Manual, Operations Manual, System Administrator Manuals, Training Materials for Branch Users, Functional Administrators and Technical Administrators, Case Studies of the proposed version of the software & USP of the proposed solution.

3. Bidder shall provide the details of SDK / API capability for customization/production configuration with flutter.

4. Vendor shall provide response to Detailed Functional & Technical Requirements specified On Annexure 1 Vendor has to furnish detailed explanation (which can be provided as a separate document by mentioning Annexure Point No) wherever it is mentioned in the Annexure Questionnaire or is required for justifying the capability of the solution. In commercial bid, vendor shall provide AMC Year to Year hike for next 5 years.

5.   Bidder shall be ready to showcase Bandwidth usage of the solution in SSL network during technical presentation of the solution using native/vanilla version of the software. Bandwidth usage obtained during technical presentation shall be taken as the benchmark value of Bandwidth for considering the solution in later stages of Negotiation. SSL will not consider bidder who is not ready to test the Bandwidth usage of it solution.

6. If the deployment model of solution proposed by vendor in both On Premise & Cloud, then separate commercials has to be shared with details of commercials for each models. For Cloud based deployment models vendor has to provide all the Audit Certifications on data center, solution, data security (along with data export at the time exit / periodical), support for all External key management solution and access control. Further any additional document required by the SSL in terms of data privacy, information security or geographic locations needs to be made available. This would not be construed as alternative to SSL's right to audit.

7. Vendor should provide the detail design of the proposed solution and also should share a detailed project plan. The plan needs to cover the UAT release dates along with SIT of individual features in a phased manner so that there won't be any delay in the UAT completion. Before each UAT release the detailed knowledge transfer needs to be completed by the Bidder at onsite location. After successful completion of all UAT phases, the application will be moved into Production Environment with all features after necessary audits. The application needs to be complied with all audit finding by SSL's empaneled auditor, Internal Audit, VAPT, Data Migration Audit or any other audit as require by SSL or regulator.

8. Vendor shall ensure to provide fixes/resolution to the issues reported during VAPT audit on an ongoing basis at no additional cost.

9. Detailed plan should include the migration of existing customer data to the new CRM Solution.

10. Data Retention needs to be implemented as per the guidelines from SSL Policy, SEBI, regulatory bodies, etc.

11. Performance testing needed to be completed and report need to be shared as part of the delivery. The product delivered should be having capability to run performance testing in UAT environment so as to ensure that each new release/customization is not having any impact on the performance of the application.

12. Bidder should ensure proper coding practices are followed and static and dynamic source code review needs to be conducted. Bidder need to share the source code review report of certified by CERT_IN Partner of the application with SSL along with UAT release or SSL will conduct source code review by CERT-IN empaneled auditor. Any customization / changes has to undergo the review of certified empaneled auditor and necessary fixes should be done by the bidder before go-live.

13. Bidder should complete the Development/Implementation of platform along with phse1 (refer annexure13 within 06 months from the date of Purchase order, if bidder is selected. Bidder shall adhere to the Warranty Period mentioned in the RFP document and post successful completion of the warranty period SSL will enter to the AMC contract(if required by SSL), with Bidder initially for 02years

14. The Hardware specifications for the SIT, UAT, Production, Pre-Production and the DR environment

needs to be provided by the bidder & should be part of solution & commercial.

15. The application should have high availability in both DC and DR. DC to DR replication also to be configured by the bidder.

16. The vendor should ensure that the platform is scalable both vertically and horizontally without any customizations in the platform. However vendor's proposed solution should be capable to handle minimum requirement given by SSL based on Concurrent of 2000 users and expected volumes in 5 years is approx. 20% year on year growth.

17. Bidder needs to support and coordinate comprehensively with the application vendor(s)/SI who is integrating (including API calls and SDK integrations) the application.

18. The bidder has to provide support and applicable patches as and when released by the OEMs connected with the proposed solution during warranty and thereafter during AMC period. Any observation raised by SSL/Regulators/Other Agencies from time to time should be rectified and fixed by the bidder within a week time after reporting without any additional cost.

19. All the integrations (API, External Web Portals, DB Integrations, etc), present in current CRM software with other sub systems has to be done in the new CRM software. All API's available within the solution has to be shared in the response along with the complete description.

20. All software should be legally purchased and necessary documents/certificates should be supplied along with the proposed solution.

21. The selected bidder should upgrade the application, whenever upgrade of OS, Middleware or DB happens due to the same going out of support, during the warranty and contract periods without any additional cost to SSL.

22. Security features should meet the standards and procedures as per SSL's Security Policies and procedures, in line with prevailing Industrial Standards including OWASP. The bidder should comply with SSL's vendor security baseline guide line. The bidder should ensure code related to the CRM solution has to be obfuscated properly with proprietary tools.

23. Ensure that the proposed solution is in compliance with regulatory requirements and other relevant regulatory guidelines. Any instances of non-compliances observed will need to be rectified well within timelines stipulated by the SSL. Incorporate changes in the system arising on impact of amendment to regulations/SSL's policy at no additional cost and well within timelines stipulated by the SSL / regulator.

24. The bidder should provide necessary admin portal and dash board required for SSL's technology/operations team with user to role/function mapping and maker checker flow.

25. Bidder shall be ready to showcase a demo of workflows in Lead Management, Customer Service Management & Campaign Management during technical presentation to SSL team.

26. Bidder shall ensure that the solution being provided is user friendly and easy to use by SSL staff. Bidder shall ensure to provide GUI Prototype/Functional Prototype as required by SSL.

5. Testing and Acceptance

SSL will conduct "User Acceptance Test" (UAT) under guidance, review and supervision of the vendor to ensure that all the functionality required by the SSL as mentioned in this SCOPE OF WORK /Requirements shared with the bidder is available and is functioning accurately as per the expectations of the SSL. Consequent to UAT, if some of the functionalities, specified in this SCOPE OF WORK are not present in tune with the SSL's expectations, the vendor shall make appropriate changes for the functioning of Solution.

The following services should be provided by the vendor:

1) Submit Test specifications, which outline the test cases, test objectives, test procedures, expected results, pass/fail criteria for each testing phases. Application Installation manual and inventory of all software deployed should be provided. Vendor will be responsible for setting and maintaining the test environment during the entire period of project implementation. The Vendor will ensure that the test environment's configuration and parameterization for conducting the UAT is in line with SSL's requirement as mentioned in this SCOPE OF WORK/Requirements shared with the bidder. The vendor should ensure that test environment has the same configuration and functionalities and it should be capable of synchronizing from production using restoration/other standard techniques functionalities as that of the live environment.

2) Bidder shall share the technical/functional delivery document, based on which business user test plan and test specifications shall be approved by the SSL before performing any tests by QA.

3) Any defects found during the tests shall be rectified or resolved within two working days by the vendor at no cost to the SSL. Re-test shall be arranged by the vendor after the rectification and the retest shall be documented. Regression testing has to be done after rectification of the defects.

4) The vendor shall be required to perform a range of unit tests for individual sub-system to demonstrate that all items have been installed and configured properly.

5) There should be another System Integration Test after the completion of all unit tests for each individual sub-system to demonstrate successful integration and error handling that the delivered solution meets all agreed features and functional requirements specified in the tender/SCOPE OF WORK.

6) The vendor shall be required to demonstrate that the delivered solution can support the workload mentioned as per expectation of SSL / as part of the requirements mentioned by SSL.

7) The vendor shall be required to demonstrate that the delivered solution can meet all the performance requirements specified e.g. the time needed in fail over.

8) The vendor will be responsible for conducting system integration testing to verify that all system elements have been properly integrated and that the system performs all its function. Vendor should support the

integration of security tools like Key Management System, HIPS, DAM, Anti - APT, SIEM/SOC PIM/PAM etc.

9) The vendor will assist the SSL in analyzing/comparing the results of testing.

10) Vendor shall provide adequate resources for troubleshooting during the entire UAT process of the SSL. After the successful completion of all the testing from vendor team, the vendor shall be required to assist SSL in performing the UAT to accept the delivered solution.

11) The vendor will be responsible for maintaining appropriate program change control and version control of the system as well as documentation of UAT and change of configuration and parameterization after making changes in the system and should be checked in to SSL's Configuration Management Tool e.g. SVN. Baseline parameter configurations should be documented and provided for OS, Middleware, and DB and Application layers.

12) Vendor shall be responsible for creating the required interfaces with the Trading Systems and other systems of SSL as per the requirements of the solution. The interfaces shall be with micro-services, API, web services, database connectivity, URLs, XML etc for both online/real-time and batch mode integrations. Suitable error logs and reconciliation systems need to be put in place wherever integrations are being built so that errors or omissions can be avoided. Suitable checks for the same may also be incorporated. Bidder should also be able to provide the reports downloadable format such as excel and PDF

13) The vendor will be responsible for using appropriate tools for logging, managing, resolving and tracking issues and its progress, arising out of testing and ensuring that all issues are addressed in a timely manner to the satisfaction of the SSL and as per the requirements mentioned. Issue Tracker shall also be made available to SSL's team.

6. Training and Documentation

1) The vendor needs to provide free trainings for all items supplied, to the SSL's technical staff, on system/application administration, configuration and entire operations of the proposed solution.

2) Training must be provided in all functional areas for sufficient duration to the satisfaction of the end users

3) Vendor will be responsible to develop training and reference materials for all the functionality of the software. Training materials should comprehensively cover all graphs, processes flows, screen-shots of the actual system functionality etc.

4) All trainings have to be conducted at the SSL's Office, unless with prior approval given by the SSL. All training sessions have to be conducted before production launch.

5) Product Certification training shall be provided by OEM mandatorily.

6) Training should be of vendor/OEM certification level standard on the delivered solution with certification training materials.

7) The training should at least cover the following areas:
- Functionality available in the solution including logic and methodology of the same
- Customization using SDK Toolkit or any other IDE

- Customization / Parameterization;
- Techniques for slicing and dicing of data, information and output;
- Advanced trouble shooting techniques if any;
- Deployment of application and identification procedures, application controls, analysis procedures provided as part of the solution;
- Monitoring & management of Webservers, Middleware's, Database as part of the solution
- Techniques of customization, development and configuration required for the solution provided;
- System and application administration such as creation/modification and deletion of user, user groups, user privilege settings, user license management, team creation, workflow creation, data import management, email configuration management, Product Configurations, analysis of application & database logs, document repository management, GUI Creation/Modification, Relationship creation for objects in CRM, System Information Security Settings etc.

8) Document deliverable include but not limited to:
   - Project plan, technical design document and product specifications.
   - Test plan, test specifications and test reports.
   - Training guide.
   - Standard product manual including software media and license materials.
   - Standard operating procedure documents.
   - Detailed installation documents
   - Issue tracker during overall project implementation.

9) Detail technical design document to be created for the development phase and proper test documentation along with approved test results to be shared with the SSL along with the UAT build.

10) Source code Audit certificate should be provided with OEM declaration that application is devoid of any malicious covert channels and free from any known bugs at the time of delivery and all subsequent releases of the proposed solution.

11) All works related to the assignment handled are to be well documented and will form the part of deliverables. They should be delivered both in hard copy and soft copy at the end of each stage.

7. Warranty & Service

The vendor shall provide three-year comprehensive warranty, extendable up to additional 2 years, out of which initial 12 months should be onsite and the remaining support can be on-site/offsite based on the decision of SSL at the closure of first year, from the date of installation of software specified in the purchase order for all the supplied products. SSL would start the implementation in the phase wise which will be intimated to the selected bidder during the finalization of the solution and the commercials will be applicable according to the go live of each module. The warranty, on-site/offsite maintenance and services/support will be provided to cover software on a 24x7 throughout the said period. Details of the warranty period of the software as per the warranty policies of the respective principals or OEM should be specified clearly along with Mode/method of support. The details of the AMC provided along with the mode of support should be clearly specified. Vendor has to offer SSL, support for the

application software by Annual Maintenance Contract (AMC) after the expiry of the warranty period if SSL is opting for the same. The scope, deliverables, time schedules and the support provided during the AMC period have to be specified clearly. Support provided to SSL during the implementation, warranty, AMC periods have to be clearly specified along with the problem escalation chart, method of support, etc.

The vendor shall sign a comprehensive Service Level Agreement with the SSL covering all relevant areas along with Purchase order. Warranty period shall be effective from the Go-Live date of the solution. Any augmented part of the solution is also covered under warranty from respective date of installations till the expiry of the Service Level Agreement. The support should cover supplied software installation, Database software, patches, bug fixes, upgrades, updates, firmware upgrades and complete maintenance of all software components throughout the warranty/support/AMC period. Support level escalation chart has to be provided for DC and DR sites.

Annual Maintenance contract / warranty / support terms must be in accordance with the SLA (Service Level Agreement) and NDA (Non-disclosure Agreement) only, notwithstanding anything contrary contained in any other documents whether executed before or after the execution of the agreements. On the happening of an incident/defect the maximum turnaround time should be defined in the SLA. The solution provided should be optimally configured such that it works at peak performance level. Any degradation in performance should be rectified by the vendor. The vendor shall absorb any hidden cost arising out of situations, with respect to services and maintenance of the complete software and related solutions offered / supplied by Vendor, which arises due to an act or omission of vendor. Vendor should take precaution to eliminate the defects to the maximum to reduce the downtime to the minimal time. A minimum uptime of 99.5% per annum is mandatory. Vendor should assist SSL in completing licensing agreements, if any with OEM's prior to commencement of warranty period. Vendor should inform compulsorily in the submitted Bid whether any licensing agreement has to be completed prior to or after delivery of any ordered item. Draft copy of such required agreement has to be submitted with the Bid. Vendor has to take full and complete responsibility for support of all supplied items.

Undertake immediate bug fix actions in the event of software failure causing an interruption of operation of the CRM application as per the response / resolution times defined in SLA. Vendor should notify about all the detected software errors and correct them in the shortest possible time. The SI/Vendor will be responsible for notification of new versions/ releases of the software and supervise their implementation in mutually agreed deadlines. Vendor should enter into the obligation that in the event OEM releases a new version of software, and SSL is using one of the previous versions, OEM would provide the full scope of services to the version used by SSL for the period of at least 5 years from the go-live date. The vendor should confirm that the software is not compromising the security and integrity of SSL's data and also not compromising the quality of operation of SSL, particularly the services rendered to customers. The vendor should support the SSL in integrating any new applications with the CRM Application. During the period of AMC, if the service provided by the bidder is not satisfactory, SSL reserves the right to terminate the AMC contract & deduction of penalties. The support shall be given in person or through telephone and E-mail within a reasonable time as the case may be. Only licensed copies of software shall be supplied and ported. Further, all software supplied

shall be of latest tested proven version which is bug free and malware free through-out the contract period without any additional cost. The Solution offered should have all components which are bug free, no malicious code, no covert channels, no known vulnerabilities reported and of latest stable version, which are having a 2 years clean track record. The Bidder shall be bound to provide technical consultancy and guidance for successful operation of the Solutions and its expansion in future by SSL during the warranty and AMC period. Preventive maintenance shall be compulsory during Warranty and AMC period. Preventive maintenance activity should be completed every quarter and report should be submitted to SSL. Preventive maintenance activity should take care of parameter configuration verification, application health check-up, fine-tuning the configuration, verification of bugs/patches etc.

8. Delivery and Installation

The application as per the purchase order specifications should be delivered in full at our Production, Pre-prod, UAT & DR, within a maximum of 06 months from the date of issuing the Purchase order along with the integration of phase 1 which will be discussed during the finalization. The timelines are to strictly adhere and any delay shall attract penalty. If the supply is delayed inordinately, SSL can cancel the said purchase deal without any obligation on its part and the same shall be binding on the vendor. Vendor should install all supplied software, including OS, database, and third party supporting software, drivers, patches and all other required software for the smooth functioning of the application / system at Data Center. Vendor should also designate a Project Manager / Leader along business analyst(s) to ensure installation and operationalization of all supplied software items. This Project Manager / Leader should be the single point contact of the SSL for its clarifications, support etc. The Name, designation, contact details of the identified Project Manager / Leader should be informed to SSL along with the SCOPE OF WORK. Vendor should submit the detailed documentation for the entire installation in both soft copy and hard copy. SSL reserves the right to involve third parties, application vendor etc., in the installation process, if it deems so and the vendor shall render all assistance for the same. Vendor should provide necessary knowledge transfer to SSL for further development and maintenance of the solution.

Penalty Clauses

The application software should be delivered within a maximum of 06 MONTHS of issuing the Letter of Intent/ Purchase order. SSL will charge penalty in the following cases

      I.   Delayed delivery/Delayed Performance
      II.   Non Delivery/Non Performance

For Category I, SSL will charge a penalty of 10% per module on the respective module purchase order value mentioned in the purchase order for delayed number of days from date of delivery stipulated/arrived at/accepted by the vendor. For Category II minimum 50% or appropriate amount/ rate for the particular module. SSL reserves the right to cancel the PO and recover the amount paid in case of the non-delivery of the module. Bidder shall ensure to adhere to the below matrix during Warranty Period and AMC period for timely resolution & response to issue reported in the Production Environment.

Issue Classification	Response Time	Resolution Time
Severity 1(Critical)	1 hour	4 hours
Severity 2(Medium)	3 hours	12 hours
Severity 3(Low)	12 hours	48 hours

9. Selection Strategy

The objective of the evaluation process is to evaluate the bids to select an effective and best fit solution at a competitive price. The evaluation will be undertaken by an Internal Selection Committee formed by the SSL. SSL may consider recommendations made by External Experts/Consultants on the evaluation. The committee or authorized official shall recommend the successful bidder to be engaged for this assignment before Board and the decision of SSL shall be final, conclusive and binding on the bidders.

SSL will scrutinize the offers to determine whether they are complete, whether any errors have been made in the offer, whether required technical documentation has been furnished, whether the documents have been properly signed, and whether items are quoted as per the schedule. SSL may, at its discretion, waive any minor non- conformity or any minor deficiency in an offer. This shall be binding on all Bidders and SSL reserves the right for such waivers and the SSL's decision in the matter will be final.

SSL may call for any clarifications/additional particulars required, if any, on the technical/ commercial bids submitted. The bidder has to submit the clarifications/ additional particulars in writing within the specified date and time. The bidder's offer may be disqualified, if the clarifications/ additional particulars sought are not submitted within the specified date and time. SSL reserves the right to call for presentation/s, product walkthroughs, on the features of the solution offered etc., from the bidders based on the technical bids submitted by them. SSL also reserves the right to conduct Reference Site Visits at the bidder's client sites. Based upon the final technical scoring, short listing would be made of the eligible bidders for final commercial bidding.

NOTE: The SSL's decision in respect of eligibility criteria, evaluation methodology and short listing of bidders will be final and no claims, whatsoever in this respect, shall be entertained.

10. Evaluation of Bid

A The proposal submitted by the Bidders shall be evaluated on the following group of parameters.

1. Functional and Technical evaluation
   - ➢ Functional Requirements (FR)
   - ➢ Technical Architecture (TA)
   - ➢ Product Demonstration and Bid Presentation (PB)
   - ➢ Approach and Methodology (AM)
   - ➢ Past Experience (PE)

2. Commercial Bid evaluation
   (Of only top 3 bidders in 1 - Functional and Technical evaluation)

Commercial Bid submitted by the vendor should be valid for a minimum period of 6 months.

3. The marks are assigned for each individual parameter under these groups and marks scored by each bidder under each parameter are aggregated to find out the total technical score of the bidder.

4. The score for evaluation of the application and the respective functionalities shall be decided by the Internal Selection Committee.

5. Bidder to submit Technical and Commercial Bid in two separate envelopes with clearly mentioning the same on the envelope.

B. Evaluation of Commercial Bid:-

For commercial bid evaluation, the SSL may consider only the top three bidders who score highest in technical and functional evaluations. The evaluation criteria mentioned in this RFP is tentative and the score earned by the bidders in accordance with the evaluation parameters set by SSL does not confer them right to be called for negotiation. Further, the SSL has sole discretion in selection of the successful bidder and decision of the SSL in this regard shall be final.

11. Award of Contract

A. Notification of Acceptance of Bid.

Before the expiry of the period of validity of the proposal, The SSL shall notify the successful bidder in writing by hand-delivery or by email, that its bid has been selected. The bidder shall acknowledge in writing receipt of the notification of selection and has to convey his absolute, unconditional and unqualified acceptance and thereafter enter into agreement / Contract within 10 days from the date on which selection is notified to bidder. The proposed format of notification of acceptance is given in Annexure-12.

B. Project Management:

➢ The bidder will nominate a Project Manager immediately on acceptance of the order, who will be the single point of contact for the project.

➢ The selected bidder shall ensure that personnel deployed are competent, do not violate any of the contractual obligations under this contract and while on the premises of the SSL conduct them in a dignified manner & shall not behave in any objectionable manner.

C. Signing of Contract

➢ Acceptance of selection shall be followed by signing of the Contract. However selection committee may negotiate certain terms & conditions with successful bidder and obtain necessary approvals from higher authorities, before signing of the Contract. The Bidders should sign the

Contract Form, which will be provided for successful bidder. The signing of Contract will amount to award of contract and Bidder will initiate the execution of the work as specified in the Contract. The signing of contract shall be completed within 15 days of receipt of notification of the acceptance of bid. Once the contract is executed, the terms in contract shall supersede the terms in the RFP.

➢ The contract is signed for the entire duration of the project. Successful bidder shall indemnify, protect and save the SSL against all claims, losses, costs, damages, expenses, action, suits and other proceedings, resulting from infringement of any patent, trademarks, copyrights etc. or such other statutory infringements under any act in force at that time in respect of all the hardware, software and network equipment's or other systems supplied by bidder to the SSL from whatsoever source.

D. Conditions Precedent to Contract

The Contract is subject to the fulfillment of the following conditions:-

➢ Obtaining of all statutory, regulatory and other permissions, approvals, consents and no-objections required under applicable laws or SEBI for the performance of the service(s) under and in accordance with the Contract.
➢ Furnishing of such other documents as SSL may specify

E. Time Period for Completion of Assignment

➢ The assignment will be for a period comprising of Implementation period 06 Months of implementing the CRM Application for SSL, Warranty period (3 years extended up to 5 years & AMC Period thereafter (Based on SSL's decision).
➢ SSL, at its option may extend the timeframe, depending on its requirements.
➢ The successful bidder shall complete the project / perform and render the Services within the agreed time frame starting from the date of award of Contract/Agreement.

F. Delay in Adhering to the Project Timelines/Liquidated Damages

➢ The Successful Bidder must strictly adhere to the time schedule, as specified in the Contract, executed between the SSL and the bidder, pursuant here to, for performance of the obligations arising out of the contract and any delay will enable the SSL to resort to any or all of the following at sole discretion of the SSL.

➢ If there is any delay in the implementation of the project due to bidder /partner's fault in complying with time schedule furnished by the bidder and accepted by the SSL, SSL will charge a penalty of 10% of module value   or will lead to cancellation of the purchase order itself. Order value cost in this context refers to total expenditure expected to be incurred by the SSL for procurement, design and implementation of CRM Application in a workable condition. Any deviations from the norms would be treated as breach of the contract by the bidder and will be

dealt with accordingly. The delay will be measured with reference to time schedule to be specified in the contract to be entered with the successful bidder.

- ➢ SSL also reserves its right to claim damages for improper or incomplete execution of the assignment.

G. Use of Contract Documents & Information

- ➢ The successful bidder shall treat all documents, information, data and communication of and with SSL as privileged and confidential and shall be bound by the terms and conditions of the Non-Disclosure Agreement. The Bidder and/or implementation partner shall execute the Non-Disclosure Agreement simultaneously at the time of execution of the Contract.

- ➢ The successful bidder shall not, without SSL's prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, sample or information or data or drawings / designs furnished by or on behalf of SSL in connection therewith, to any person other than a person employed by the Bidder in the performance of the Contract.

- ➢ Any document in any form it has been obtained, other than the Contract itself, enumerated in this Bid Documents shall remain the property of SSL and shall not be returned.

12. General Terms & Conditions

12.1 Confidentiality

This document contains information confidential and proprietary to SSL. Additionally, the Bidder will be exposed by virtue of the contracted activities to internal business information of SSL, the Associates, Subsidiaries and/or business partners. The Bidders agree and undertakes that they shall keep confidential all matters relating to this RFP and will not make any disclosure to any person who is under the obligation under this document, any information, data, and know-how, documents, secrets, dealings, transactions or the terms or this RFP (the "Confidential Information"). Disclosure of receipt of this RFP or any part of the aforementioned information to parties not directly involved in providing the services requested could be treated as breach of confidentiality obligations and SSL would be free to initiate any action deemed appropriate. The restrictions on disclosure of confidential information shall not apply to any matter which is already available in the public domain; or any disclosures made under law.

No news release, public announcement, or any other reference to this RFP or any program there under shall be made without written consent from SSL. Reproduction of this RFP, without prior written consent of SSL, by photographic, electronic, or other means is strictly prohibited.

12.2 Non-Disclosure Agreement

The shortlisted bidder will be required to sign a Non-Disclosure Agreement with SSL as per the annexure. The Bidder shall treat all documents, information, data and communication of and with SSL as privileged and confidential and shall be bound by the terms and conditions of the Non-Disclosure Agreement.

"Receiving Party", which expression shall, unless repugnant to the context or meaning thereof, be deemed to include its successors and permitted assigns). This should also include all the employees / promoters/ directors of the company.

12.3 Governing Law and Jurisdiction

All disputes and controversies arising out of this RFP and related bid documents shall be subject to the exclusive jurisdiction of the Courts in Mumbai and the parties agree to submit themselves to the jurisdiction of such court and the governing law shall be the laws of India.

12.4 Arbitration

All disputes and differences of any kind whatsoever shall be settled by Arbitration in accordance with the provisions of Arbitration and Conciliation Act, 1996 or any statutory amendment thereof. The dispute shall be referred to the sole arbitrator who shall be appointed by SSL. The venue of Arbitration proceedings shall be at Mumbai. The Arbitration proceedings shall be conducted in English Language. The award of the Arbitration shall be final and binding on both the Parties and shall be delivered in Mumbai in the English language. The fees of the Arbitrator and the cost of the Arbitration proceedings shall be equally borne by both the Parties.

12.5 Indemnification

The Bidder shall, at its own cost and expenses, defend and indemnify SSL against all losses, judgments, statutory and regulatory penalties, fines, damages, third-party claims on account of the any misrepresentation, infringement of intellectual property rights, fraud and breach of terms of this RFP/ violation by the Bidder of any or all national/international trade laws, norms, standards, procedures etc.

The Bidder shall expeditiously meet any such claims and shall have full rights to defend itself there from. If SSL is required to pay compensation to a third party on account of the Bidder or association with the Bidder, then the Bidder shall be fully responsible for the same, including all expenses and court and legal fees.

12.6 Force Majeure

In case of delay in implementation of the Project on account of conditions which are beyond the control of the shortlisted bidder such as war, floods, earthquakes, strikes, lockouts, epidemics, pandemic, riots, fire or Governmental regulations superimposed after the date of order/ contract, the Parties shall be permitted to terminate the contract / bid document, if such delay extends for a period beyond 15 days. SSL shall not be liable to make any payments in this case.

12.7 Termination

SSL reserves the right to abandon the current tender process and restart the bidding process at any point of time without assigning any reason whatsoever. SSL can cancel the award granted to the elected Bidder at any point of time and restart the bid process completely or select another Bidder. The Elected Bidders understands and agrees that SSL shall not be obligated in any manner whatsoever and is free to stop / modify the bidding process at any stage without any liability.

12.8 Data Protection

The Bidders authorizes the release from time to time to SSL (and any of its Subsidiaries or Affiliates) all personal or professional data that is necessary or desirable for the administration of the RFP (the "Relevant Information"). Without limiting the above, the bidders permit SSL to collect, process, register and transfer to and aforementioned entities all Relevant Information. The Relevant Information will only be used in accordance with applicable law.

12.9 Intellectual Property

SSL shall have sole exclusive ownership to all its Intellectual property including and not limited to its trademarks, logos etc. This RFP shall in no way be considered as a transfer or assignment of the respective rights over any intellectual property owned, developed or being developed by SSL.

Annexure

Check List for Submission of Bid Documents

Sr. No	Description	Annexure No.
1	Functionality Response Document	1
2	Check list for Submission of Eligibility Criteria	2
3	Profile of Bidder/Partner	3
4	Implementation Methodology	4
5	Reference Site Details	5
6	Past Experience	6
7	Cover Letter for Commercial Bid	7
8	The format for furnishing the price of Software & Hardware	8
9	Table for Arriving at the Total Cost*	9
10	Bid Submission Covering Letter	10
11	Notification of Acceptance	11
12	Performance Certificate	12
13	Payment Terms	13
14	Bid Evaluation Methodology	14
15	Non-Disclosure Agreement	15

*Annexure – 9 to be submitted in a separate envelope subscripting as "COMMERCIAL BID" and all other annexures in a separate envelope subscripting as "TECHNICAL BID".

Please note that submission of Commercial and Technical Bid in a single envelope or submission of annexure- 9 or copy of it along with technical documents in the envelope subscribed as "TECHNICAL BID" may lead to rejection of the Bid and disqualification of bidder for this RFP.

Annexure 1   Functionality Response Document

Vendor is requested to furnish the appropriate response to the particulars asked by giving the compliance level as explained below. Explanations/suggestions by the vendor may be given in the Remarks column. If more explanation of a point is needed, documents can attach to the Remarks Column in any section.

Availability Type	Description
A	Already Available FULLY in the product.
B	Not Available but can be provided. Should be included in the version of the product being supplied before implementation. (Free of charge)
C	Functionality requires customization of the product
D	Not Feasible in the product due to architecture or structural limitations.

Note:
All the points updated with Availability Type A, B, C are to be mandatorily delivered along the proposed CRM solution to SSL without any additional cost.

1. Functional Requirements

Sr no.	Module	Module / functionality need classification (Must have / Good to have)	Module availability	Solution description and details	Availability Type	Total Score
1	Lead management - Provides an overview of leads, and describe the different options for creating leads across all business verticals, managing them, and working with them throughout their lifecycle.	Must have				
2	Customer 360 view - The module collates & stores customer information including transaction history or behavioural actions across multiple systems to get a complete picture of the customer for gaining better insights and the ability to take actions with this information. This includes the entire lifecycle of the customer from on-boarding till exit along with cross product details.	Must have				
3	Customer dashboards - Module provide a visual compilation of the customer/business data and insights captured in customer 360 view. Dashboards should be configurable as per user profile. eg: CSE should be able to view all open cases across all business verticals, productivity for the day of the support agent / Dealer RM, AHT etc. along with the	Must have				

	integration with IVR & other interaction channels which will be part of solution					
4	Reports & analytics - The module help to gain key business insights and provide reports to help understand customers, business measures and key performance indicators. Track case life cycle at each stage from creation, tagging, assignment, reassignment, closure	Must have				
5	Admin module - e.g. RBP (role based permission) and User creation etc. - Module provide access to its users based on predefined role and function matrix based on roles and responsibilities at various user levels. Modification of drafts, scripts and changes in tagging should be available with SSL admin without dependency on external person.	Must have				
6	Ticket management system - Module helps to track individual customer service issues across channels / business vertical and agents over time.	Must have				
7	Telephonic integration - Module will establish computer- telephony integration to initiate outgoing calls, receive and forward incoming calls directly in CRM and also get a profile screen showing their customer information	Must have				

	Provide time bound alerts for call-backs (calendar integration)					
8	Customer voice - Module allows immediate capture of feedback across channels with personalized surveys to continuously track customers' perception of services and products.	Must have				
9	Alerts and trigger management - Module is used to automate key processes to create follow-up items, alerts, emails or trigger additional internal or external processes.	Must have				
10	Engagement tool (Emails, SMSs, Chatbot and WhatsApp) - Module helps in contacting customers on-the-move with targeted promotional messages, appointment and invoice notifications on their preferred communication channel	Must have				
11	Reputation experience management - Module monitors user reviews & feedback for the products & services over social media platforms and assist users in resolving their issues through timely responses to their posts / feedback thus improving customer experience	Must have				
12	Live chat & chatbot - Module helps communicate with the customers through live chat and chat bot (for initial communication via virtual agent)	Must have				

13	Automated workflow - Module provides visually defined workflow to rapidly design and automate any business process with drag-and-drop simplicity Assignment of emails based on given logics (keyword, write backs, ageing, HNI flag etc.)	Must have					
14	Knowledge management - Module provide team members the ability to author, categorize, deliver, analyse, and share information through a knowledge base	Good to have					
15	Campaign management Module helps in planning, execution, tracking, and analysis of all initiative	Must have					
16	Omni channel support - Module help customer service handle their customers by offering a variety of support channels such as phone support, email, live chat etc	Must have					
17	Agents' presence information - Module helps to determine if a work item can be routed to the agents depending on their location and availability	Good to have					
18	Defining agents' capacity - Defining capacity(utilization) of agents across channels for assisting in case assignments	Must have					
19	Message templates - Allows for ensuring that standard communications are being sent across to customers from all the members of the organization	Good to have					
20	Monitor real-time customer satisfaction -	Must have					

	Assist agents in understanding how a customer is feeling, real-time sentiment is displayed when the agent is having a conversation with the respective customer					
21	Agent Modules - (scripts, Assists, Dashboard, Collaboration) - Allows agents to collaborate with other agents and supervisors, while working with any customer, provides the agents with guidance to ensure that they are using the best process for resolving customers' issues, provides real-time recommendations to agents to help them take actions while interacting with customers	Must have				
22	File attachment capability - Support agent and customers to send needed/supporting files as per SSL Policy & Guidelines	Must have				
23	Conversation transcripts - This module allows customers to download or receive an email copy of their chat transcripts	Good to have				
24	Social messaging channel - An instant way to connect with customers online, functioning as an always-on channel, one that customers control and can dip in and out of	Must have				
25	Customer service insights across business verticals - The module makes use of AI and analytics capabilities to proactively improve the customer satisfaction by	Must have				

	offering better insights and data based future predictions					
26	Conversation insights - Help sales managers and sellers in their day-to-day job, providing the tools they need to track their sales performance in calls with leads and customers	Must have				
27	Forecast management - This module helps to predict how much revenue the sales team will generate in a given time frame	Good to have				
28	Sales sequence model - This module helps salespeople get familiar with best practices and operate according to the business processes	Good to have				
29	Contact management & business card scanner - Module helps scan business cards, create and store contacts	Good to have				
30	Opportunity management - The module help manage opportunities and typically includes several customer interactions such as meetings with the customer, phone calls, or tasks	Must have				
31	Goal management - This module is used to track your goals across teams and analyze the results of your goal management to make better business decisions	Must have				
32	Self-service Module(QMS): Customer should be able to get answers to their most asked questions on platforms for unanswered queries					

should be able to send their query to the Customer Service team. Request ID should get auto created and assigned to Customer Service team for action. Customer should be able to view the status of their request at any point along with resolution provided. Also, the Help section created should be in multiple languages along with API which will by other solutions for integration with KMS (Knowledge management Solution) proposed					

2. Technical Requirements

I. Integration Capability

Sr no.	Module	Availability Type	Module availability	Solution description and details	Total Score
1.1	Ability to integrate with relevant applications/IVR Telephony for Service Request/Lead Management/Campaign Activity/Customer 360				

1.2	Ability to integrate with Email gateway (SMTP service & Server level Email Authentication) and SMS Gateway(through DB/API's interfaces)				
1.3	Ability to interface with third party applications via Web Services (REST/SOAP) and ISO communication ,SQL queries(Orade, SQL Server, MySQL DB)				
1.4	Ability to integrate with directory services standards like LDAP(Microsoft Active Directory) & 2 FA solution for user authentication and password change/reset				
1.5	Availability of integration toolkit/SDK/Standard IDE as out of box for customization by SSL's Team without the need of separate customization.as part of CRM platform at no additional license or product cost. (The SDK should be compatible with Flutter)				
1.6	Whether Source code of customizations will be shared with SSL'				
1.7	Whether Product Source code will be shared with SSL for code review and customization.				
1.8	Ability to create/modify GUI fields by Frontend by admin user				

1.9	Ability to modify and create GUI layout/dashboard/User Screen and adding validations/java scripting by the admin user				
1.10	Capability to integrate with Partner's CRM for leads and complaint management of third party products.				
1.11	Ability to integrate with Social Media Platform(Facebook, Whatsapp, Twitter, Instagram,etc) & Chatbot solution through native API's supported in the platforms and availability of OOB(Out of the Box) plugins for Integration.				
1.12	Integrate with API's for Lead Management & Customer Service Request Management.				

II. Data Migration

Sr no.	Module	Availability Type	Module availability	Solution description and details	Total Score
2.1	Ability to migrate the CRM data of Leads & Service Request from existing Solution(CRM Next)				
2.2	Migrate existing API's and interfaces in Lead and Service Management Module for integrating with other applications like Website, Mobile App etc.				
2.3	Capability to carry out Migration Audit to make sure that all the data from existing CRM solution is completely migrated to the new system and to prevent any data loss during migration.				

III.Mobility

Sr no.	Module	Availability Type	Module availability	Solution description and details	Total Score
3.1	Availability of Native Mobile App of CRM in Android & IOS Platforms				
3.2	Availability of Customer 360, Sales and Service Module as Out of Box Modules in Mobile Client without any additional customizations				
3.3	Ability to publish the changes in real time to Mobile Client whenever any update/patch is deployed on the CRM Web Application				

3.4	Compatibility of Mobile Client with latest Android OS & IOS versions				
3.5	Ability to add/modify GUI fields by admin user				
3.6	Ability to configure separate layout for pages in Mobile Client				
3.7	Ability to configure custom dashboards in Mobile Client based on User roles				
3.8	Ability to add custom workflow for sales users in Mobile Client				
3.9	Ability to integrate AD authentication for user login in Mobile Client				
3.10	GPS tracking & Geo - Tagging sales user of Mobile Client				
3.11	Ability to perform route planning for the RM going out for meetings				
3.12	Ability to work offline, and then automatically synchronizes data bi - directionally once a connection has been re – established				
3.13	Option to create tasks, Easily manage and enter account info., Add and organize contacts, Schedule meetings: Transmit meeting notes or details at the point of contact, Assign follow up activities, Track existing or new opportunities, Request approvals, chats, KPI's for target & reporting.				

Sr no.	Module				
3.14	Facility to enable Sales Users automatically create, process, and route the sales orders they receive to ensure rapid fulfilment, even if they're not in the office				
3.15	Ability to control the mobile device access of CRM and provides access and relevant data to authorized individuals only and with encryption, authentication, and authorization technologies and role based services				

IV. CRM Data import

Sr no.	Module	Availability Type	Module availability	Solution description and details	Total Score
4.1	Availability of ETL Tool as out of box with the CRM solution				
4.2	Ability of Data Import mechanism to extract data from different Data Bases(Oracle, SQL Server, MySQL etc) and Feed files(plain text, spreadsheet)				
4.3	Specify the Data Import mechanism with details on mechanism of data transfer(Web Services/SQL/MSMQ etc)				
4.4	Specify the Benchmark on no of records that can be inserted to CRM solution per hour				

4.5	Specify the standard Benchmark of the solution for Data loading				
4.6	Specify the models available to load daily incremental data load and real time data loading mechanism				
4.7	Capability to schedule and configure data lading process in batch job mode/real time by admin users from GUI				
4.8	Capability of loading complete customer data from core system to CRM Solution as one time process and benchmark on the maximum no for records loaded/hour.				
4.9	Availability of Error Handling mechanism in Data Import Process during data import/scheduling process and ability to handle run time exception during Data Import.				
4.10	Option available as out of box feature to generate reconciliation report after the daily run of data import by comparing with records in the source tables/feed files				

V, Licensing model and upgrades

Sr no.	Module	Availability Type	Module availability	Solution description and details	Total Score
5.1	Specify different Licensing Model of the CRM				

	Application (Enterprise/User License/Both)				
5.2	No separate licenses shall be needed in SIT, DR & UAT environments. Specify Nature of (Perpetual/Subscription) license				
5.3	Any separate master agreement to be executed with OEM for Licensing				
5.4	Specify Model of Solution Upgrade & Mobile Client for next 5 years				
5.5	All product upgrades can be implemented in DC/DR sites along with all environments without any additional cost to SSL during AMC period Whether all security updates based on Audit from Regulatory/External agencies shall be provided without any additional cost				
5.6	Enterprise License Cost (Applicable if vendor is offering for Enterprise Licensing Model)				
5.7	Per license cost for users, bulk user costs and packages as applicable				

VI. Architecture/General

Sr no.	Module	Availability Type	Module availability	Solution description and details	Total Score

6.1	Specify the model of deployment of the solution (On Premise/Cloud/Hybrid).If the proposed solution is supporting in Cloud and On-Premise models, it can be mentioned separately in response.				
6.2	Specify whether Physical Server/VM is supported for Deployment				
6.3	Detailed list of OS/DB/Middleware/Webserver/Application Platform & any other supporting software/license to be procured by SSL for implementation, however the commercials to be included in the commercial bid.				
6.4	Specify Hardware Specifications needed with Architecture Diagram, Network Diagram, Schema Design, and Functional Specification Document of the solution for proposed implementation. (In hardware details, Mention the no of CPU Cores, memory etc). The commercials for the hardware, if on-prem, will have to be included in the commercials.				
6.5	Benchmark on minimum Bandwidth(in kbps) required for accessing the application smoothly Specify the Web Server, Application Platform & DB Details				
6.6	Benchmark on maximum Bandwidth (in kbps) required for accessing the application smoothly. In case of bandwidth usage varies based on different modules, share the value in kbps for each modules like Customer 360, Lead Module, Service Module, and Campaign Module				
6.7	Product Customization Certification Training shall be provided by OEM				

6.8	Benchmark on Solution Performance in terms of CPU, Memory, application Page load time etc.				
6.9	Specify List of Supported Browsers for accessing the solution with Base version details in each browser (MS Edge, & Chrome).				
6.10	Specify the End of Life of present version of software proposed				
6.11	Specify the mode of Data Security of the application available				
6.12	Ability to encrypt Personal Identifiable information (PII) of Customer Data in Database along with integration with external Key Management Solution. PII data should be masked in all front end views.				
6.13	Specify whether VDI Solution (e.g.: Citrix) is needed for accessing the solution from branches with bandwidth of 512 kbps.				

VII. API needs and integration touch points

Sr no.	Module	Availability Type	Module availability	Solution description and details	Total Score
7.1	Following CRM API's shall be delivered from the solution apart from the standard Native API's present i. Lead Creation ii. Lead Update iii. Lead Closure iv. Lead Escalation v. Lead Interaction Update vi. Lead Details View vii. Lead Status View viii. Bulk Lead Import ix. Bulk Lead Closure x. Case (Service Request) Creation xi. Case Updation xii. Case Escalation xiii. Case Status View xiv. Case Details View				

xv. Case Closure xvi. Create Child Case xvii. Closure of Child Case xviii. Case Interaction Update xix. Customer Interaction Update xx. Get Customer Details – To Fetch Customer Details xxi. Create Campaign Response xxii. Create Marketing List (Input will contain the marketing list records) xxiii. Update Marketing List xxiv. Update Campaign Details xxv. Contact Creation (Customer/Non Customers)					

7.2	List of integrations needed to be mentioned: • SMTP - Email Integration. • SMSC - SMS Integration. • Telephonic Integration. • SBI Securities Mobile App. • SBI Securities Customer Portal. • Data lake/DWH integration. • Account opening system. • Dealer advisory system. • Whatsapp Integration. • DP integration TEAM integration. • Firebase Cloud Messaging integration (to send push notifications). • HRMS Integration. • Core Application **Furthermore 10-15 integrations to be considered**					

VIII. Workload

Sr no.	Module	Availability Type	Module availability	Solution description and details	Total Score
8.1	Ability to handle concurrent 2000 users in the CRM application				
8.2	Ability to handle large volume of email, whatsapp and SMS messages to be sent from Application say for an average monthly volume of 1 crore with growth of 10% per year.				

IX. Cloud Security Checklist

Bidders have to comply with the below checklist if the solution proposed is on cloud:

Control No	Control Category	Controls to be implemented	Compliance status
1	Asset Management	Is there a comprehensive list of cloud assets and services being maintained for cloud services and SAAS applications procured	
2	Asset Management	Are the cloud assets classified as per business criticality and severity	
3	Asset Management	Are there controls to monitor and classify cloud services and applications that host sensitive PII and business data?	
4	Asset Management	Whether there are controls to ensure sensitive PII data or business data is not transmitted outside the cloud environment in a secured manner	
5	Cloud Security Controls	Whether the cloud assets deployed are hardened using security baselines? Or whether the services hosted are using pre - hardened baseline images?	

6	Cloud Security Controls	For any deviations to the security baselines, is there a deviation preapproved with the CISO and Business team?	
7	Cloud Security Controls	Whether access to virtual servers and cloud services are restricted to designated administrators? Is the access control for these access defined on a "Need to Know" or "Need to Have" basis	
8	Cloud Security Controls	Whether cloud environments have been segregated virtually into Production, UAT and Development zones?	
9	Cloud Security Controls	Whether access to virtual server consoles and services are restricted to administrators only?	
10	Cloud Security Controls	Whether backups of virtual server images and deployment templates are being stored in a secured manner & the export of the data can be done to SSL in a readable format.	
11	Cloud Security Controls	Whether disaster recovery is in place for cloud services and applications hosted to ensure availability of application services across various availability zones	
12	Cloud Security Controls	Whether administrative access around creation, deletion and modification to cloud servers and services being logged and monitored on an ongoing basis	
13	Cloud Security Controls	Is there a provision to report cloud services related incidents as part of the current incident management process	
14	Cloud Security Controls	Whether periodic training is being provided to resources on security risks and usage of cloud services	
15	Cloud Security Controls	Check whether the CASB controls have been implemented to secure access to Applications, API services and accounts managed over the cloud	
16	Cloud Security Controls	Check whether the CASB logs are integrated with SIEM to monitor and alert abnormal user behaviour on the cloud operations around unauthorized data transfer, data downloads, malware uploads, etc on cloud	

17	Cloud Security Controls	Check for integration of CASB tools with threat intelligence tools for up-to-date intel on unauthorized IP sources or access to cloud environment	
18	Cloud Security Controls	Whether ongoing monitoring of user activities and operations is being carried out in an automated manner for cloud assets for user accounts review, health monitoring, concurrent sessions etc.	
19	Cloud Security Controls	Check whether appropriate SLAs are defined to ensure compliance to timely resolution of incidents	
20	Cloud Data Security	Whether data classification is performed of the cloud assets and services which are hosted	
21	Cloud Data Security	Whether appropriate encryption and security controls are in place to restrict access to sensitive PII data in the cloud environment	
22	Cloud Data Security	Whether information is being retained as per the retention requirements specified as part of the data retention requirements	
23	Cloud Data Security	Are there appropriate controls in place to restrict data movement using secured SSL channels or secured services while deployed into cloud	
24	Cloud Data Security	Whether data backups and snapshots created for the cloud assets are stored in an encrypted form using cryptographic keys	
25	Cloud Data Security	Whether DLP controls are implemented for IAAS services to restrict movement of sensitive data outside the cloud environment	
26	Cloud Data Security	Whether controls are in place to restrict usage of production data into UAT / Staging without data masking / anonymization	
27	Cloud Data Security	Whether a proper key management process is being followed for key generation, key implementation across services, key storage, key distribution and key destruction activities	
28	Cloud Data Security	Whether keys generated have a defined time frame to ensure re-generation of cryptographic keys on regular interval	

29	Cloud Data Security	Whether data volumes, databases, PAAS and IAAS services are encrypted prior to hosting and processing any sensitive data on cloud	
30	Cloud Data Security	Whether any data deletion activities performed is carried out through crypto shredding mechanisms. Also integration with external Key management Solution is possible or not.	
31	Cloud Identity and Access Management	Whether access to cloud services and applications hosted are managed through centralized Identity and Access Management solution	
32	Cloud Identity and Access Management	Whether Role based accesses have been defined for application and infrastructure teams to ensure least privilege access to cloud services on a need to have basis	
33	Cloud Identity and Access Management	Whether Privileged Identity to IAAS services are managed through PIM based solutions	
34	Cloud Identity and Access Management	Whether third party access which are being reviewed for applicability in a timely manner?	
35	Cloud Identity and Access Management	Whether user access roles on cloud assets and applications have been segregated based on functional roles, segregation of critical activities and operational responsibilities	
36	Cloud Identity and Access Management	Whether strong authentication and password controls have been implemented as part of cloud services and applications.	
37	Cloud Identity and Access Management	Whether network segmentation has been implemented to segregated based on different trust zones for cloud servers and services	
38	Cloud Identity and Access Management	Whether access to Virtual Private Cloud (VPC) and APIs Gateways are restricted to cloud administrators only for management and operations. Explain how the restrictions are being made	
39	Cloud Identity and Access Management	Whether access to cloud services and applications and management are routed through secure network controls such as IP whitelisting, Ssl VPN, MDM solution, etc	
40	Cloud Identity and Access Management	Whether access to cloud services and accounts are restricted using 2FA authentication controls?	

41	Cloud Identity and Access Management	Whether critical and sensitive applications, VPC Services and data do not have any direct interface from internet?	
42	Cloud Identity and Access Management	Whether adequate controls are in place to restrict direct updates to cloud database and application data?	
43	Cloud Risk Assessment, Threat Intelligence and Vulnerability Management	Whether regular risk assessments are being carried out at least annually for the business and cloud security risks applicable as part of the cloud operations	
44	Cloud Risk Assessment, Threat Intelligence and Vulnerability Management	The cloud services and activity logs are integrated with SSL's SIEM tool for continuous security monitoring and incident identification. Bidder to confirm on various SIEM tools compatible	
45	Cloud Risk Assessment, Threat Intelligence and Vulnerability Management	Whether ongoing vulnerability assessments are being performed at least on a defined frequency on a biannual frequency	
46	Cloud Risk Assessment, Threat Intelligence and Vulnerability Management	Whether the vulnerabilities identified are being tracked and rectified in a timely manner	
47	Incident Response and Management	Check whether there are process control measures to identify data breaches or incidents which have being identified through external sources	
48	Incident Response and Management	Incidents are being recorded as part of the incident management process along with the RCA	
49	Incident Response and Management	Whether the current incident processes are equipped to identify cloud services related incidents as part of the ongoing process	
50	Cloud Data Centre	The SaaS Provider shall confirm if the data centre is located within India and approved by MEITY empaneled Cloud Service Providers.	

Bidder to submit the compliance adherence to the circular SEBI/HO/ITD_VAPT/P/CIR/2023/033

X.   API Security

Bidders to submit the details of the various API's available and confirm on the below compliance:

Control No.	Control area	Requirements	Compliance status
1	Application Security	Channel Encryption:	
2	Application Security	Payload Encryption:	
3	Application Security	List of Data consumed by API:	
4	Application Security	Authentication and authorization techniques used : Tokens generated per secret keys from Dashboard - evidence	
5	Application Security	Source authentication in API (what is the authentication mechanism used to authenticate clients) Token based - evidence	
6	Application Security	Rate limiting in API:	
7	Application Security	Access restrictions to API:(is it accessible from Internet or Is Firewall rule given to specific customers only)	
8	Application Security	Details of Logs collected by API:	
9	Application Security	Data flow diagram for end-to-end data usage by API from API client to DB	
10	Application Security	Detailed Documentation on how the data uploaded by API is consumed	
11	Application Security	Protection of system test data	
12	Application Security	Document/ SOP for communication between application service (API) information processing interoperability	
13	Application Security	Evidence to show Application interface to cloud service customers are provided so that they programmatically retrieve the data to enable interoperability and portability	

Sl. No.		SLA with cloud service customers (if any) to show customers can access data upon contract termination including:		
14	Application Security	SLA with cloud service customers (if any) to show customers can access data upon contract termination including: a. Data format, b. Length of time the data will be stored, c. Scope of the data retained and made available to the cloud service customers and d. Data deletion policy?		

Annexure 2   Check List for Submission of eligibility criteria

Sl. No.	Details	Compliance (Yes/ No)	Proofs to be enclosed	Remarks (avoid this column during submission)
1	Bidder should be a company under Indian Laws.			Reference of Act/Notification, Registration Certificate or any document evidencing the formation of entity and full address of the registered office.
2	The bid shall be submitted by either an OEM (Original Equipment Manufacturer/ Product Vendor) / SI (System Integrator). The term "bidder" used in this RFP refers to the entity who has submitted the bid.			Certificate from OEM for SI as Bidder.
3	Bidder should be a profitable organization for the last 3 years and should have turnover of at least INR 50 Crores for the last financial year.			Copy of the audited balance sheets along with Profit and Loss statement for the corresponding years and / or Certificate of the Chartered Accountant.
4	The bidder should be a company and have a local presence of support center locally in India.			Bidder should specifically confirm on their letter head in this regard.
5	The Authorized Partner / Distributor / SI, etc. also should have direct presence or representative offices and support centers in India.			Bidder should specifically confirm on their letter head in this regard.

6	3 Client references of the implementation in India should be provided for a similar deployment.			Client Details with Email/Landline/Mobile for whom the Bidder has executed similar projects. This should include the Bank to whom this solution has been provided. The bidder should also provide performance certificate (clients letterhead Annexure-13) from clients kept as reference (Start and End Date of the project to be mentioned) 1. 2. 3.
7	Bidder should not have been blacklisted for deficiency in service			Self-Declaration to be submitted by the bidder, which is subjected to the satisfaction of SSL
8	Past/Present litigations, disputes, if any			Brief details of litigations, disputes, if any are to be given on Company's letter head.
9	Development / Testing/ Deployment Methodologies			Documents on development/ testing / deployment framework, tools, templates & utilities

10	If the bidder intends to partner with another entity to complete the entire assignment, they should clearly specify in the bid the name of that entity (i.e. OEM/SI) with whom they propose to partner. Further the bid should clearly spell out the tasks proposed to be undertaken by the partner. If any of the functional/technical requirements is achieved with the help of partner, details of such requirements shall be mentioned in the bid and during the product demonstration the partner shall display his capability in achieving the aforementioned requirements. The partner is also required to fulfill the eligibility criteria specified in this RFP and the bidder is responsible for furnishing the required details to check the eligibility of partner. No subcontracting is allowed.			Bidder should specifically confirm on their letter head in this regard.
11	Bidder should sign the Non-Disclosure Agreement in stamp paper.			
12	Successful Bidder should execute SLA with SSL before the start of project execution.			Bidder should specifically confirm on their letter head in this regard.

Annexure-3 Profile of bidder/Partner

Profile of bidder/Partner

	Particulars	Response
1	Company Name	
2	Date of Incorporation	
3	Name of Indian representative/office (indicate: own, dealer, distributor,)	
4	Company Head Office address * Contact person(s) * Designation * Phone Number * Mobile Number * E-mail Address	
5	Address of Indian representative/office * Contact person(s) * Phone Number * E-mail Address	
6	Number of Employees supporting the project : * Marketing/Sales * Technical Support * Research and Development * Implementation	
7	Ownership structure (e.g. Inc., partnership) * Who are the primary shareholders? * State the major shareholders with percentage holding in case of limited Companies.	
8	Years of Experience in Providing the CRM Solution to the clients	

9	Location: Support Location – In India	
10	Provide the range of services offered covering service description and different schemes available for: Customization, Implementation Support, Delivery Ongoing support (AMC, Help Desk), Training Any Others (specify)	
11	State pending or past litigation if any within the last year with details and Explain reasons. Please also mention any claims/complaints received in the last year.	
12	Enclose abstracts of the Balance sheet and P/L Account for the last year	
13	Independent analyst research report (if any)	
14	Major changes in Management for the last year	

Annexure-4   Implementation methodology

Sl. No	Details of methodology / approach
1	The methodology section should adequately address the following stages of the project:
i.	Frequency and approach for periodic reporting on the progress of the project and actual status vis à vis scheduled status
ii.	Detailed Study of Current State, with detailed work steps and deliverables
iii.	Gap analysis including identification and resolution of gaps
iv.	Customization, development and necessary work around
v.	Building up of interfaces with the applications used by SSL
vi.	Setting up of the platform and deploying the CRM Application for SSL/ Other relevant applications.
vii.	SIT, User acceptance testing, Performance testing
viii.	Pre Go-live Audit, Data Migration audit, VAPT,WASA, Delivery Audit
ix.	Planning for rollout and identification of key issues that may arise along with proposed solutions
2	Timelines
3	Project management activities
4	Roles and responsibilities of proposed personnel both from the vendor and SSL end.
5	Following details with respect to the methodology followed by the vendor in Project Management for a SSL
i.	Project Name

ii.	Project Location
iii.	Client Name
iv.	Client address
v.	Client contact/reference person(s)
vi.	Project started (month/year)
vii.	Project elapsed time – months
viii.	Man months effort
ix.	Project Size (No of branches, modules covered and any other relevant details)
x.	Name of senior project staff
xi.	Nature of the Project
xii	Project Management Methodology used
xiii.	Role of the Bidder, whether complete end to end involvement or for a particular module
xiv.	Project detail (Broad detail – information about all activities handled, modules forming part of the Project of the Client , associated activities, time lines, Activity wise and module wise may be detailed.)

Annexure-5   Reference Site Details

The reference sites submitted must be necessarily of those BFSI (Broking preferred) firms where the proposed Bidder/Proposed software solution has been awarded the contract in the last three years prior to the last date for submission of bids at SSL. For those references where the offered solution is accepted but implementation is not started, the acceptance should be valid as on the last date for submission of bids at SSL. Please provide reference details in the format defined below:

Particulars	Response
Name of the firm Country of Operation	
Address of the Organization	
Annual Turnover of the Organization for the Financial Year 2022-23	
Date of commencement of Project	
Date of completion of Project	
Scope of Work for Solution	
Partner for the project	
Project Start date and End date	
List all the modules/components of the system being used.	
Type of Architecture in which the system has been implemented.	
Implementation details e.g. Number of Sites, time taken for Operationalization, volumes of processing etc.	
State the duration of the implementation	

Number of users and the geographical spread of the implementation	
Average Team size on site for project implementation (SI & OEM Team)	
Contact Details from the firm for reference	
Name of the Contact Person	
Designation	
Phone Number/e-mail	

Annexure-6   Past Experience

List of major customers where the proposed solutions have been implemented/under implementation and their reference details

No.	Name complete Postal Address of the Customer	Name & Brief scope of work done by OEM	Name & Brief scope of work done by SI (Specify the size of the Firm, the Approaches supported etc.)	Attach Reference Letter	Contact Details (Name, Designation, Phone, Email)	Project Status(Completed/Under Implementation, Start Date, End Date)

(Enclose necessary documentary proof such as reference letter etc.)

Annexure-7   Cover Letter for Commercial Bid

Note: This Cover Letter for Commercial Bid from the Bidder should be on the letterhead of the Bidder and should be signed by an authorized person.

Date:

To, Trushita T/Paren S (IT – Department)

SBICap Securities LTD

Address- Marathon Futurex

12th Floor ,B wing

N M Joshi Marg, Lower Parel (East)

Mumbai :- 400013

Dear Sir/ Madam,

Subject: Response to RFP Ref No: XXXXXXXXXXXXX

Having examined the Bidding Documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to supply & deliver the CRM Application inconformity with the said Bidding documents may be ascertained in accordance with the commercial bid (termed as Annexure- 9 and Annexure-10 in your RFP) attached herewith and made part of this Proposal.

We undertake, if our Proposal is accepted, to deliver, install and commission the system, in accordance with Requirements specified within the RFP and as per the Best Practices and Guidelines of SEBI and other relevant Acts, rules, regulations, directions as applicable.

We agree to abide by the Proposal and the rates quoted therein for the orders awarded by SSL.

Until a formal contract is prepared and executed, this bid, together with your written acceptance thereof and your notification of award shall constitute a binding Contract between us.

We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws in force in India.

We understand that you are not bound to accept the lowest or any Proposal you may receive. Dated this

.... day of 2023

....   (Signature) (In the capacity of)

Duly authorized to sign bid
for & on behalf of (Name &
Address of the Bidder)

Annexure-8   **Format for furnishing the price of Software/Hardware (Bill of Material)**

a.   <u>**The format for furnishing the price of software**</u>

SSL intends to procure CRM Application. SSL should have the ownership and right to use these without any restriction of modification.

SI No	Item	Unit Price in INR	Description	Total Price in INR	Comments by Vendor
1					
2					

Note: Applicable taxes and Duties:
Details of all applicable taxes to be paid by the SSL must be specified like sale tax, service tax etc. Applicable Duties to include customs, Excise etc. All taxes and duties to be given in Rupee value only.

Dated……

(Signature)

(In the capacity of)

Duly authorized to sign bid for & on
behalf of (Name & Address of
the Bidder)

Annexure-9   **Table for Arriving at the Total Cost**

TABLE-A: Cost of the application, License, Hardware, Customization, Change Request (Per Man day cost), FM support fees, Training, etc.

Sl.No	Item Description	Unit Price	Total Price	Taxes / VAT if any	Total payable

GRAND TOTAL

Note: In case of application cost, separate cost Split up shall be shared on Module wise (eg: Customer 360, Sales Management, Service Management, Campaign Management, License Cost etc.)

TABLE-B: Cost of AMC after the warranty for Software, Customization etc

SL No.	Item Description	AMC Amount for full period after warranty (Year wise)	Service Taxes if any	Total payable
	Grand Total			

(Amount in INR only)

TOTAL PAYABLE IN INDIAN RUPEES AS PER TABLE A	
TOTAL PAYABLE IN INDIAN RUPEES AS PER TABLE B	
TOTAL BID PRICE.	

Amount in words:
Dated……

(Signature) (In the capacity of)

Duly authorized to sign bid for & on behalf of (Name & Address of the Bidder)

Annexure-10   **Bid Submission Covering Letter**

Note: This Bid Offer Covering letter should be on the letterhead of the Bidder and should be signed by an authorized person.

Date:

To,

<mark>Trushita T/Paren S</mark> (IT – Department)

SBICap Securities LTD

Address- Marathon Futurex

12th Floor ,B wing

N M Joshi Marg, Lower Parel (East)

Mumbai :- 400013

Dear Sir/ Madam,

Subject: Response to RFP Ref No: **XXXXXXX**

i.   With reference to the RFP, having examined and understood the instructions, terms and conditions forming part of the RFP.
ii.   We agree and undertake that, if our Bid is accepted, we shall deliver, install and commission the CRM Application in accordance with the Requirements specified within the RFP within the timeframe specified, starting from the date of receipt of notification of award from SSL.
iii. We acknowledge having received the following addendum to the bid document:

Addendum	Date

➢ All the details mentioned by us are true and correct and if SSL observes any misrepresentation of facts on any matter at any stage, SSL has the absolute right to reject the bid / proposal and disqualify us from the selection process.

➢ We confirm that the offer is in conformity with the terms and conditions as mentioned in RFP and it shall remain valid for 180 days from the last date of the acceptance of this bid.

➢ We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws in force in India.

➢ We are also aware that SSL has also right to re-issue / recommence the bid, to which we do not have right to object and have no reservation in this regard; the decision of SSL in this regard shall be final, conclusive and binding upon us.

➢ We confirm that our company/system integrator/other partners participating in this bidding as part of the consortium have not been black listed/banned by a regulatory authority and

any previous ban is not in force at present.

Dated this .... day of 2023

Yours faithfully,

(Signature)

(In the capacity of)Duly authorized to sign bid for & on behalf of

(Name & Address of the Bidder)

Annexure-11   Notification of Acceptance

<u>(On Organization's letter head)</u>

Place:

Date:

To,

SBICap Securities LTD

Address- Marathon Futurex

12th Floor ,B wing

N M Joshi Marg, Lower Parel (East)

Mumbai: - 400013

Dear Sir,

SUB: RFP No **XXXXXXX**

REF: Your Letter No: -_____Dated_____.

This has reference to your letter on the subject, notifying us about the selection of our bid.

We hereby convey our absolute, unconditional and unqualified acceptance for the work and activities as per the Scope of Work and other terms and conditions mentioned in the subject RFP.

Signature of Authorized
Person (Seal)

Annexure-12 Performance Certificate

To be provided on Organization's letter head

To,

SBICap Securities LTD

Address- Marathon Futurex

12th Floor ,B wing

N M Joshi Marg, Lower Parel (East)

Mumbai :- 400013

Sir,

Reg.: RFP for CRM Solution

This is to certify <company Name with Address>has supplied/implemented Complete CRM solution originally developed by <OEM name> in our organization since <Month and Year>. The CRM solution is running successfully in our organization and the services of <company Name >are satisfactory.

The solution is handling transaction volume of approx. <xxx> TPS.

The certificate has been issued on the specific request of the <company Name >.

Place: Date:

Signature of Authorized

Signatory Name of

Signatory:

Designation:

Email ID:

Mobile No:

Telephone

No.:

<Seal of Bank/Client>

Annexure 13   Implementation Phases

- Phase 1 :Complete platform to be implemented with Customer service enablement, integration with Contact centre, email integration and data migration from the current platform
- Phase 2 : Lead Generation, Data integration, Customer 360, Marketing and Analytics / Reporting to be completed within 3 months post Phase 1 sign off.

Annexure 14   Payment Terms

- Software / License Cost of the Product on Delivery and Acceptance -90%- (30% Against UAT Setup, Balance 60% post sign off in proportion to the respective module go live)
- Software / License Cost of the Product on submission of Performance Bank Guarantee-10%
- One Time Implementation Cost On Successful completion of Implementation and Project Signoff and complete migration-100%

Annexure-15   Bid Evaluation Methodology

SL No.	Evaluation Points	These are the parameter the Bidder will be evaluated, Bidder to update details
1	**Features**	
	1) Existing feature mentioned in the Business Requirement Document	
	2) Value additions Bidder can provide other than the requirements shared by SSL	
	Annexure 2	
2	Architecture	
3	Product Demonstration & Bid presentation	
4	Approach and Methodology	
5	Time line to complete the Project(it is an added advantage for the bidder to complete the project within 3-6 months	
6	Past Experience	

1) How many years Bidder is doing CRM application development	
2) Years of Experience in BFSI domain	
3) How many clients Bidder is serving with CRM application	
4) Experience in Migrations in BFSI	

Annexure 16   Non-Disclosure Agreement (NDA)

(To be printed on Bidder's Letter Head and included with the Technical Bid Envelope)

THIS AGREEMENT ("the Agreement") is made on this _____ day of _____, 2022.

BETWEEN

SSL, an Indian company duly incorporated under the Companies Act, 1956, having its registered office at Marathon Futurex, 12th Floor, B Wing, N. M. Joshi Marg, Lower Parel, Mumbai – 400 013 (hereinafter for the purposes of this agreement, referred to as "SSL"/ "Disclosing Party"), which expression shall, unless repugnant to the context or meaning thereof, be deemed to mean and include its successors and permitted assigns;

AND

_____LIMITED, a company incorporated Registered under the Companies Act, 1956 and having its registered office at _____ _____

_____ in (hereinafter referred to as the "Receiving Party"), which expression shall, unless repugnant to the context or meaning thereof, be deemed to include its successors and permitted assigns)

WHEREAS:

1. SSL is   registered with SEBI as a Stock Broker and a Depository Participant and distributing third party financial products including mutual funds/Tax Free bonds and is registered with Association of Mutual Funds in India (AMFI).

2. The Receiving Party is engaged in the business of _____.

3. SSL and the Receiving Party are in the process of discussion and negotiation wherein SSL will provide its Information related to Systems, Device, Applications, logs, etc. ("Information") to the Receiving Party and may in the course of discussion, negotiation and/or performance of the said Services, disclose,

provide or make available to the Receiving Party certain Confidential Information as defined herein below, and

4. SSL desires to restrict use and disclosure of such Confidential Information as set out herein below.

NOW THEREFORE in consideration of the mutual promises and covenants contained in this Agreement, and the mutual disclosure of Confidential Information to each other, the Parties hereto agree as follows:

1. Confidential Information and Confidential Materials

(a) "Confidential Information" means non-public information that SSL designates as being confidential or which under the Confidential Information circumstances surrounding disclosure ought to be treated as confidential. "Confidential Information" includes, without limitation, information relating to released or unreleased SSL's services or products, the marketing or promotion of any SSL Product, SSL's business policy, Confidential Information or practices, and information received from others that SSL is obligated to treat as confidential. Confidential Information disclosed to the Receiving Party by any parent or agent of SSL, or by any subsidiary of parent of SSL, is covered by this Agreement.

(b) Confidential Information shall not include any information that: (i) is or subsequently becomes publicly available without the Receiving Party's breach of any obligation owed to SSL; (ii) became known to the Receiving Party prior to SSL's disclosure of such information to the Receiving Party; (iii) became known to the Receiving Party from a source other than the breach of an obligation of confidentiality owed to SSL; (iv) is independently developed by the Receiving Party.

(c) "Confidential Materials" shall mean all tangible materials containing Confidential Information, including without limitation, written or printed documents and computer disks or tapes, whether machine or user readable, the Software being licensed including any manual and documents relating to the Software, its Source Code, etc.

2. Restrictions

(a) Except as provided below, the Receiving Party shall not disclose any Confidential Information to third parties. However, the Receiving Party may disclose Confidential Information in accordance with judicial or other governmental order, provided the Receiving Party shall give SSL reasonable notice prior to such disclosure and shall comply with any applicable protective order or equivalent. This restriction on disclosure of Confidential Information shall apply to all the Confidential Information disclosed before entering the service agreement and shall continue to have effect during the subsistence of the Service Agreement. It shall also survive the termination of such agreement for provision of the services, as set out in the recitals hereinabove.

(b) The Receiving Party shall take reasonable security precautions, at least as great as the precautions it takes to protect its own confidential information, to keep confidential the Confidential Information. The Receiving Party may disclose Confidential Information or Confidential Material only to the Receiving Party's employees or consultants on a need-to-know basis. The Receiving Party will have executed or

shall execute appropriate written agreements with its employees and consultants sufficient to enable it to comply with all the provisions of this Agreement

(c) Confidential Information and Confidential Materials may be disclosed, reproduced, summarized or distributed only in pursuance of the Receiving Party's business relationship with SSL, and only as otherwise provided hereunder. The Receiving Party agrees to segregate all such Confidential Materials from the confidential materials of others in order to prevent commingling.

(d) Publications: the Receiving Party shall not make any news releases, public announcements, give interviews, issue or publish advertisements or publicize in any other manner whatsoever in connection with this Agreement, the contents / provisions thereof, other information relating to this Agreement, the Purpose, the Confidential Information or other matter of this Agreement, without the prior written approval of the SSL.

3. Rights and Remedies

(a) The Receiving Party shall notify SSL immediately upon discovery of any unauthorized use or disclosure of Confidential Information and/or Confidential materials, or any other breach of this Agreement by the Receiving Party, and will co-operate with SSL in every reasonable way to help SSL to regain possession of the Confidential Information and/or Confidential Materials and prevent its further unauthorized use.

(b) The Receiving Party shall return all originals, copies, reproductions and summaries of Confidential Information or Confidential Materials at SSL's request, or at SSL's option, certify destruction of the same.

(c) The Receiving Party acknowledges that monetary damages may not be a sufficient remedy for unauthorized disclosure of Confidential Information or Confidential Materials and that SSL shall be entitled, without waiving any other rights or remedies, to such injunctive or equitable relief as may be deemed proper by a court of competent jurisdiction.

4. Miscellaneous

(a) All Confidential Information and Confidential Materials are and shall remain the property of SSL or any affiliate thereof. By disclosing information to the Receiving Party, SSL and/or its affiliate(s) do not grant any express or implied right to the Receiving Party to or under any patents, copyrights, trademarks, or trade secret information.

(b) Any software, product, service and documentation provided under this Agreement is provided with RESTRICTED RIGHTS.

(c) Terms of confidentiality under this Agreement shall not be construed to limit either party's right to independently develop or acquire products without use of other party's Confidential Information. Further, either party shall be free to use for any purpose the residuals resulting from access to or work with such Confidential Information, provided that such party shall maintain the confidentiality of the Confidential Information as provided herein. The term "residuals" means information in non-tangible form, which may be retained by persons who have had access to the Confidential Information, including the ideas, concepts, know-how or techniques contained therein. Neither party shall have any obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of residuals. However,

the foregoing shall not be deemed to grant to either party a license under the other party's copyrights or patents.

(d) This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. It shall not be modified except by written agreement dated subsequent to the date of this Agreement and signed by both Parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of SSL, its agents, or employees, but only by an instrument in writing signed by an authorized officer of SSL. No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.

(e) This Agreement shall be governed by and construed in accordance with the laws of India and shall be subject to the exclusive jurisdiction of the courts of Mumbai.

(f) Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the Parties, their successors and assigns.

(g) If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect.

(h) All obligations created by this Agreement shall survive change or termination of the parties' business relationship.

(i) In the event this Agreement (including any schedules, exhibits or attachments hereto) is signed in both the English language and in any another language, any conflict or inconsistency between the different language versions shall be resolved solely by reference to the English language version.

5. Arbitration

All the disputes in connection with this Agreement, the construction of any provision of this agreement or the rights, duties or liabilities of the parties hereto under this Agreement shall be amicably settled. However, in the event of any such disputes are not settled amicably between the Parties, reference shall be to three arbitrators. Each party shall appoint its Arbitrator and the two respective Arbitrators appointed by each party shall appoint a presiding Arbitrator to adjudicate the dispute, difference, claim, etc. between the parties. A Party wishing to refer a dispute to arbitration shall appoint its arbitrator and send notice of such appointment in writing to the other party requiring the other party to appoint its own arbitrator within 30 calendar days of that notice and stating that it will appoint its arbitrator as sole arbitrator unless the other party appoints its own arbitrator and gives notice that it has done so within the 30 days specified above. If the other party does not appoint its own arbitrator and give notice that it has done so within the 30 days specified, the Party referring a dispute to the arbitration may, without the requirement of any further prior notice to the other party, appoint its arbitrator as sole arbitrator and shall advise the other party accordingly. The award of such sole arbitrator shall be binding on both parties as if he had been appointed by agreement.

The arbitration will be held in Mumbai, India and will be conducted in the English language.

IN WITNESS WHEREOF, THE PARTIES HERETO HAVE CAUSED THIS AGREEMENT TO BE EXECUTED AS OF THE DAY AND YEAR FIRST ABOVE WRITTEN

SIGNED AND DELIVERED   )

For SSL   )

)

In the presence of:)

1.   )

2.   )

SIGNED AND DELIVERED   )

For _____Limited   )

In the presence of:)

1.   )

2.

3.