भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

Request for Proposal for supply and installation of Web Application Firewall

RFP Reference No: NPCI/RFP/2018-19/IT/17 dated 25.02.2019
National Payments Corporation of India
Unit no. 202, 2nd floor,
Raheja Titanium, CTS No. 201,
Western Express Highway,
Goregaon East, Mumbai 400 063
Website: www.npci.org.in

Copyright Notice
Copyright© 2019 by National Payments Corporation of India. All rights reserved.

Disclaimer

The information contained in this Request for Proposal (RFP) document or information provided subsequently to Bidder or applicants whether verbally or in documentary form by or on behalf of National Payments Corporation of India (NPCI), is provided to the Bidder on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is not an offer or invitation by NPCI to any parties other than the applicants who are qualified to submit the Bids ("Bidders"). The purpose of this RFP document is to provide Bidder with information to assist the formulation of their Proposals. This RFP document does not claim to contain all the information each Bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP document and where necessary obtain independent advice. NPCI makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP document. NPCI may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP document.

Note: Bids will be opened in the presence of the Bidders' representatives who choose to attend Bid opening meeting.

Checklist

The following items must be checked before the Bid is submitted:

1. Demand Draft / Banker's Cheque / Bank Guarantee of INR 5,00,000/-(Rupee Five Lakhs only) towards Bid Security in Envelope 'A'- Earnest Money Deposit (EMD)
2. Eligibility Criteria, Technical and Commercial Bids are prepared in accordance with the RFP document.
3. Envelope 'A'- Eligibility Criteria Response.
4. Envelope 'B'- Technical Response
5. Envelope 'C'- Commercial Bid.
6. All the pages of Eligibility Criteria Response, Technical Bid and Commercial Bid are duly sealed and signed by the authorized signatory.
7. RFP document duly sealed and signed by the authorized signatory on each page is enclosed in Envelope – 'A'.
8. Prices are quoted in Indian Rupees (INR).
9. All relevant certifications, audit reports, etc. are enclosed to support claims made in the Bid in relevant Envelopes.
10. All the pages of documents submitted as part of Bid are duly sealed and signed by the authorized signatory.
11. Prices should be quoted individually for all categories
12. NPCI reserves rights to choose any quantity.

Abbreviations and Acronyms

The following abbreviations and acronyms defined in this RFP are as under

BG	Bank Guarantee
DC	Data Centre
EMD	Earnest Money Deposit
IPR	Intellectual Property Rights
LAN	Local Area Network
NPCI	National Payments Corporation of India
OEM	Original Equipment Manufacturer
RFP	Request for Proposal
PBG	Performance Bank Guarantee
SAN	Storage Area Network
SLA	Service Level Agreement
WAN	Wide Area Network
WAF	Web Application Firewall

Section 1 - Bid Schedule and Address

Sr. No.	Description	Detailed Information
1	Name of Project	RFP for supply and installation of Web Application Firewall
2	Tender Reference Number	NPCI/RFP/2018-19/IT/17
3	Date of release of this RFP	25.02.2019
4	Last date and time for receiving Bidder's Pre-Bid clarifications in writing	01.03.2019
5	Date and Time for Pre Bid Meeting	NA
6	Last date and time for Bid Submission	08.03.2019 05.00 pm
7	Address of Bid Submission	National Payments Corporation of India, Unit no. 202, 2nd Floor, Raheja Titanium, CTS No. 201, Western Express Highway, Goregaon East, Mumbai 400 063
8	Date and Time of Eligibility bid (Envelope A) and Technical bid (Envelope B) opening	08.03.2019 05.30 pm
9	Date and time of Commercial bid Opening (Envelope C)	Technically qualified bidders would be informed
10	Name and Address for Communication	Head - IT Procurement National Payments Corporation of India, Unit no. 202, 2nd Floor, Raheja Titanium, CTS No. 201, Western Express Highway, Goregaon East, Mumbai 400 063
12	Bid Related Queries	Satya Kanungo Contact: 8108108658 Email Id : satya.kanungo@npci.org.in Samuel Thiyagarajan Contact: 8291970845 Email Id : samuel.thiyagarajan@npci.org.in Prashant Awale Contact: 8108108650 Email id : prashant.awale@npci.org.in Benny Joseph Contact: 8108122844 Email id : Benny.joseph@npci.org.in Nolan Dsouza Contact: 7506446552 Email id : nolan.dsouza@npci.org.in
13	Bid Cost	Rs.11,800/- (Rs.10,000.00 plus applicable GST@18%) (Bid cost should be in Indian Rupees only)
14	EMD/Bid Security	Rs 5,00,000 (Rupees Five Lakhs)

Note:
1. Bids will be opened in the presence of the Bidders' representatives who choose to attend.
2. Date and Time & Address for Commercial Bid opening will be intimated later to the qualified Bidders.

Section 2 - Introduction

2.1 About NPCI

National Payments Corporation of India (NPCI) is a Company registered under Section 25 of the Companies Act, 1956 (corresponding to Section 8 of The Companies Act, 2013) with its Registered Office in Mumbai, India. NPCI was promoted by 10 banks in India under the aegis of the Indian Banks" Association with majority shareholding by Public Sector Banks. Presently 56 banks are shareholders of NPCI. Out of which 19 are Public Sector Banks (PSB), 17 Private Sector Banks, 3 Foreign Banks, 7 Multi State Cooperative Banks and 10 Regional Rural Banks.

The vision, mission and values of NPCI are: Vision - To be the best payments network globally, Mission - Touching every Indian with one or other payment services and to make our mission possible, we live and work by five core values: Passion for Excellence, Integrity, Customer Centricity, Respect and Collaboration.

2.2 Objective of this RFP:

NCPI intends to deploy Web Applications Firewall (WAF) solution in NPCINet environment to protect the most critical applications of NPCI like UPI. NPCI using WAF deployment targets to project these key applications from any web related attacks that may hit its application from various partners' connection to application via NPCINet.

This objective of this RFP is to highlight and identify a System Integrator in order to achieve the following objectives:

- Provide a secure environment to protect web applications against attacks and data leakage
- Safeguard application-layer traffic through signatures and acceptable-use profiles.
- Protect the servers from exposure

2.3 Cost of the RFP

The Bidder shall bear all costs associated with the preparation and submission of its bid and NPCI will, in no case, be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

The Bidders can submit the bid response at NPCI's office at Unit no. 202, 2nd floor, Raheja Titanium, CTS No. 201, Western Express Highway, Goregaon East, Mumbai 400 063.

2.4 Due Diligence

The Bidders are expected to examine all instructions, terms and specifications stated in this RFP. The Bid shall be deemed to have been submitted after careful study and examination of this RFP document. The Bid should be precise, complete and in the prescribed format as per the requirement of this RFP document. Failure to furnish all information or submission of a bid not responsive to this RFP will be at the Bidders' risk and may result in rejection of the bid. Also the decision of NPCI on rejection of bid shall be final and binding on the bidder and grounds of rejection of Bid should not be questioned during/after the final declaration of the successful Bidder.

The Bidder is requested to carefully examine the RFP documents and the terms and conditions specified therein, and if there appears to be any ambiguity, contradictions, inconsistency, gap and/or discrepancy in the RFP document, Bidder should seek necessary clarifications by e-mail as mentioned in Section-1.

2.5 Ownership of this RFP

The content of this RFP is a copy right material of National Payments Corporation of India. No part or material of this RFP document should be published in paper or electronic media without prior written permission from NPCI.

Section 3 – Scope of Work

3.1 Scope of work:

The scope of work will broadly include supply, installation solution and subsequent maintenance and support. NPCI intends to procure following solution and the broad scope of work will include but not limited to the following:

- Provision of a centralized management system to manage WAF devices across both NPCI locations.
- Web application firewall hardware appliance for DC & DR
- Ensure High availability setup for WAF devices at both NPCI locations.
- Availability of minimum 2 Gbps of WAF throughput at each location. This throughput should be delivered by the proposed solution when all features are turned on and WAF is in blocking mode.
- The bidder should migrate to new setup with no/minimum downtime as possible.
- The bidder should fine-tune all WAF policies based on the application requirements.
- The bidder should perform a detailed configuration assessment after 1 year from date of installation.
- The bidder should provide OEM product hands on training at NPCI location as per terms specified by NPCI.
- The bidder shall submit the project details in MS project (MPP based).
- Ensure one-time implementation of the above solution

Updates/ Version upgrades of all software components provided by bidder for 3 years without any extra cost.

Detailed Scope of Work

1. WAF Appliance – 04 Nos. as active-active for two DC
2. The WAF solution should support all standard and latest web browsers
3. All appliances/hardware and software offered is required to be on-premises licensed to NPCI. Bidder is required to Size all the hardware/software for the solution proposed. During the warranty period of the appliance/hardware or software, in case of any shortfall of software licenses or Hardware sized; bidder is required to provide software / hardware at no additional cost to NPCI.
4. The solutions deployed should be modular, scalable and should be able to address NPCI requirements for the next three years, with the deployed hardware.
5. The solutions and services in scope should be designed with adequate redundancy and fault tolerance to ensure compliance with SLAs for uptime as outlined in this RFP.
6. The solutions should not have a significant impact on the existing infrastructure of the NPCI either during installation or during operation of the solutions.
7. The Bidders who wish to take up the project shall be responsible for the following (as applicable based on the specific scope of work for the participating NPCI):
    - Procurement of the necessary solutions and the corresponding hardware, software, database etc. required for implementing these solutions at the NPCI.
    - Implementation of the identified solutions at NPCI including configuration, customization of the products as per the requirement. Also, implemented solution must meet NPCI's system security requirements.

- Solution will be installed by Bidder, pursuant to the Request for Proposal (RFP) document relating to providing of the implementation, training and assessment services.
- Bidder will engage in providing design, installation, configuration, UAT, transfer of information and assessment of the solution to NPCI.
- Development of operating procedures in adherence to security policy of NPCI.
- Bidder to specify the need of VM or other hardware for storage or hosting of application. Also, to mention rack, cable, space, power and storage required to host in-scope solutions. The bidder shall provide the year wise requirement of storage at both DC & DRS if required.
- NPCI will provide the network based on mentioned bandwidth requirement by bidder for the in-scope solution. It is expected that the proposed solution should consume minimal bandwidth, so that it should not impact NPCI day to day business operations.
- NPCI will provide the required Ethernet switch ports. However, bidder is required to mention the number of Ethernet switch ports required for in- scope solution.
- The bidder shall provide the detailed technical architecture comprising of hardware (including configuration) with operating systems and other application software in their technical bid.
- In case the bidder has not indicated any peripherals /equipment in their proposed solution and these may be required for the successful implementation of the Information Security Awareness solution, the successful bidder has to provide the required peripherals/equipment at no additional cost to NPCI.
- Bidder shall apply all software updates / version upgrades released by the respective OEMs during the contract period.
- The Bidder shall provide on call / onsite OS support on a need basis throughout the contract period starting from the date of installation and configuration

3.2 Single Point of Contact

The selected Bidder shall appoint a single point of contact, with whom NPCI will deal with, for any activity pertaining to the requirements of this RFP.

Section 4 - Instruction to Bidders

4.1 Eligibility Criteria

The Eligibility Criteria are furnished below:

1. The bidder is a Company registered under the Companies Act/ Partnership / LLP at least since last three years.
   a. In case the bidder is the result of a merger / acquisition, at least one of the merging companies should have been in operation for at least 3 years as on date of submission of the bid.
   b. In case the bidder is the result of a demerger / hiving off, at least one of the demerged company or resulting company should have been in operation for at least 3 years as on the date of submission of bid.

2. The bidder should have reported minimum annual turnover of Rs. 10 Crores as per audited financial statements in each of the last three financial years (i.e.2015-2016, 2016-2017 & 2017-2018) and should have reported profits (profit after tax) as per audited financial statements in at least two of last three financial years (i.e., 2015-2016, 2016-2017 & 2017-2018). In case audited financial statements for 2017-2018 are not ready, then management certified financial statement shall be considered for 2017-2018, however, this exception is not available in case of previous financial years. In case of a JV / Consortium / Strategic partnership, the bidder should have reported profits as per above criteria.
   a. In case the bidder is the result of a merger / acquisition, due consideration shall be given to the past financial results of the merging entity for the purpose of determining the net worth, minimum annual turnover and profit after tax for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 3 years. For this purpose, the decision of NPCI will be treated as final and no further correspondence will be entertained on this.
   b. In case the bidder is the result of a demerger / hiving off, due consideration shall be given to the past financial results of the demerged company for the purpose of determining the net worth, minimum annual turnover and profit after tax for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 3 years. For this purpose, the decision of NPCI will be treated as final and no further correspondence will be entertained on this.

3. The bidder should be authorized to quote for the OEM products and support. Further, the bidder shall submit the declaration stating that bidder will not remain associated with this RFP in any other capacity as a part of distribution channel provided such bidder has become eligible for commercial evaluation as per this RFP.

4. The Bidder should not be currently blacklisted by any bank / institution in India or abroad.

Section 5 - Instruction to Bidders

A. The Bidding Document

5.1 RFP

RFP shall mean Request for Proposal. Bid, Tender and RFP are used to mean the same.

The Bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the Bidding document. Submission of a bid not responsive to the Bidding Document in every respect will be at the Bidders risk and may result in the rejection of its bid without any further reference to the bidder.

5.2 Cost of Bidding

The Bidder shall bear all costs associated with the preparation and submission of its bid, and NPCI will in no case be responsible or liable for those costs.

5.3 Content of Bidding Document

The Bid shall be in 3 separate envelopes, Envelope A, B and C.

5.4 Clarifications of Bidding Documents and Pre-bid Meeting

A prospective Bidder requiring any clarification of the Bidding Documents may notify NPCI in writing at NPCI's address or through email any time prior to the deadline for receiving such queries as mentioned in Section 1.

Bidders should submit the queries only in the format given below:

Sr. No.	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	Additional Remarks (if any)

Replies to all the clarifications, modifications received through mail and email will be posted on NPCI's website. Any modification to the bidding documents which may become necessary shall be made by NPCI by issuing an Addendum.

5.5 Amendment of Bidding Documents

1. At any time prior to the deadline for submission of bids, NPCI may for any reason, whether at its own initiative or in response to a clarification requested by a Bidder, amend the Bidding Documents.

2. Amendments will be provided in the form of Addenda to the Bidding Documents, which will be posted in NPCI's website. Addenda will be binding on Bidders. It will be assumed that the amendments contained in such Addenda had been taken into account by the Bidder in its bid.

3. In order to afford Bidders reasonable time to take the amendment into account in preparing their bids, NPCI may, at its discretion, extend the deadline for the submission of bids, in which case, the extended deadline will be posted on NPCI's website.

4. From the date of issue, the Addenda to the tender shall be deemed to form an integral part of the RFP.

B. Preparation of Bid

5.6 Bid Price

Prices would be exclusive of all taxes. The bidder shall meet the requirements of the applicable Goods & Services Tax (GST).

5.7 Earnest Money Deposit (EMD)

The Bidder is required to deposit Rs 5, 00,000/- (Rs Five Lakhs only) in the form of a Demand Draft / Pay order in favor of "National Payments Corporation of India" payable at Mumbai or Bank Guarantee issued by a scheduled commercial bank valid for six months, with a claim period of 12 months after the expiry of validity of the Bank Guarantee as per the statutory provisions in this regard, as per format in Annexure A1 or A2.

No interest will be paid on the EMD.

5.8 Return of EMD

The EMDs of successful Bidder/s shall be returned / refunded after furnishing Performance Bank Guarantee as required in this RFP.

EMDs furnished by all unsuccessful Bidders will be returned on the expiration of the bid validity / finalization of successful Bidder, whichever is earlier.

5.9 Forfeiture of EMD

The EMD made by the bidder will be forfeited if:

a) Bidder withdraws its bid before opening of the bids.
b) Bidder withdraws its bid after opening of the bids but before Notification of Award.
c) Selected Bidder withdraws its bid / Proposal before furnishing Performance Bank Guarantee.
d) Bidder violates any of the provisions of the RFP up to submission of Performance Bank Guarantee.
e) Selected Bidder fails to accept the order within five days from the date of receipt of the order. However, NPCI reserves its right to consider at its sole discretion the late acceptance of the order by selected Bidder.
f) Bidder fails to submit the Performance Bank Guarantee within stipulated period from the date of execution of the contract. In such instance, NPCI at its discretion may cancel the order placed on the selected Bidder without giving any notice.

5.10 Period of Validity of Bids

Bids shall remain valid for a period of 180 days after the date of bid opening as mentioned in Section 1 or as may be extended from time to time. NPCI reserves the right to reject a bid valid for a period shorter than 180 days as non-responsive, without any correspondence.

5.11 Extension of Period of Validity

In exceptional circumstances, prior to expiry of the bid validity period, NPCI may request the Bidders consent to an extension of the validity period. The request and response shall be made in writing. Extension of validity period by the Bidder should be unconditional and irrevocable. The EMD provided shall also be suitably extended. A Bidder may refuse the request without forfeiting the bid Security.

5.12 Format of Bid

The bidder shall prepare two copies (one hard copy marked as ORIGINAL and one soft copy) of the Technical Bid only. In case of any discrepancy between them, the original shall govern.

The commercial bid will be submitted as hard copy only.

5.13 Signing of Bid
The Bid shall be signed by a person or persons duly authorized to sign on behalf of the Bidder.

All pages of the bid, except for printed instruction manuals and specification sheets shall be initialed by the person or persons signing the bid.

The bid shall contain no interlineations, erasures, or overwriting, except to correct errors made by the Bidder, in which case such corrections shall be initialed by the person or persons signing the Bid.

The bid shall be signed by a person or persons duly authorized to bind the bidder to the contract. Such authority shall be either in the form of a written and duly stamped Power of Attorney (Annexure G) or a Board Resolution duly certified by the Company Secretary, which should accompany the Bid.

C. Submission of Bid
5.14 Envelope bidding process
The Bid shall be prepared in 3 different envelopes, Envelope A, Envelope B and Envelope C.

Each of the 3 Envelopes shall then be sealed and put into an outer envelope marked as **'Request for Proposal for supply and installation of Web Application Firewall'.**

The inner and outer envelopes shall be addressed to NPCI at the address mentioned in Section 1.

The inner envelopes shall indicate the name and address of the Bidder.

If the outer envelope is not sealed and marked as indicated, NPCI will assume no responsibility for the bids misplacement or premature opening.

5.15 Contents of the 3 Envelopes
Envelope A - Eligibility Bid
The following documents as per the sequence listed shall be inserted inside Envelope A:

1 Bid Earnest Money in the form of Demand Draft - Annexure A1 **OR** Bid Earnest Money in the form of Bank Guarantee – Annexure A2
2 Bid Offer form (without price) – Annexure B
3 Bidder Information – Annexure C
4 Declaration of Clean Track Record – Annexure D
5 Declaration of Acceptance of Terms and Conditions – Annexure E
6 Declaration of Acceptance of Scope of Work – Annexure F
7 Power of Attorney for signing of bid – Annexure G
8 Eligibility Criteria Matrix – Annexure H along with supporting documentary proof for each criterion as stipulated.
9 OEM/Manufacturer Authorization Letter – Annexure I
10 Three years audited Balance Sheet and Profit and Loss Statements.
11 RFP document duly sealed and signed
12 All necessary supporting documents

Envelope B - Technical Bid
The following documents shall be inserted inside Envelope B:

1 Section 11 – Technical Requirements duly completed - Annexure K
2 Client Reference - Annexure L along with **supporting documentary evidence**
3 OEM/Manufacturer Authorization Letter – Annexure I
4 Entire commercial bid with **price masked**(**Annexure M**, **N** and **L** with **masked price**)

Envelope C - Commercial Bid

1 Commercial Bid Form – Annexure M
2 Commercial Bid – Annexure N
3 Detailed Bill of Material – Annexure O

5.16 Bid Submission
The Bidder should bear all the costs associated with the preparation and submission of their bid and NPCI will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

Bids sealed in accordance with the Instructions to Bidders should be delivered at the address as mentioned in the Section 1.

The offers should be made strictly as per the formats enclosed.

No columns of the tender should be left blank. Offers with insufficient/inaccurate information and Offers which do not strictly comply with the stipulations given in this RFP, are liable for rejection.

5.17 Bid Currency
All prices shall be expressed in Indian Rupees only.

5.18 Bid Language
The bid shall be in English Language.

5.19 Rejection of Bid
The bid is liable to be rejected if the bid document:

a) Does not bear signature of authorized person.

b) Is received through Fax / E-mail.

c) Is received after expiry of the due date and time stipulated for Bid submission.

d) Is incomplete / incorrect.

e) Does not include requisite documents.

f) Is Conditional.

g) Does not conform to the terms and conditions stipulated in this Request for Proposal.

No bid shall be rejected at the time of bid opening, except for late bids and those that do not conform to bidding terms.

5.20 Deadline for Submission
The last date of submission of bids is given in Section 1. However the last date of submission may be amended by NPCI and shall be notified through its website.

5.21 Extension of Deadline for submission of Bid
NPCI may, at its discretion, extend this deadline for submission of bids by amending the bidding documents which will be intimated through NPCI website, in which case all rights and obligations of NPCI and Bidders will thereafter be subject to the deadline as extended.

5.22 Late Bid
Bids received after the scheduled time will not be accepted by the NPCI under any circumstances. NPCI will not be responsible for any delay due to postal service or any other means.

5.23 Modifications and Withdrawal of Bids
Bids once submitted will be treated, as final and no further correspondence will be entertained on this.

No bid will be modified after the deadline for submission of bids.

5.24 Right to Reject, Accept/Cancel the bid
NPCI reserves the right to accept or reject, in full or in part, any or all the offers without assigning any reason whatsoever.

NPCI does not bind itself to accept the lowest or any tender and reserves the right to reject all or any bid or cancel the Tender without assigning any reason whatsoever. NPCI also reserves the right to re-issue the Tender without the Bidders having the right to object to such re-issue.

5.25 RFP Abandonment
NPCI may at its discretion abandon the process of the selection of bidder at any time before notification of award.

5.26 Bid Evaluation Process
The Bid Evaluation will be carried out in 2 stages:

Stage 1 – Envelope 'A' i.e. Eligibility bid and **Envelope 'B'** i.e. Technical bid will be evaluated. Only those Bidders who have submitted all the required forms and papers and comply with the eligibility and technical criteria will be considered for further evaluation.

Stage 2 -Envelope 'C' i.e. Commercial bids of the short listed Bidders who qualify after Technical Evaluation only will be opened.

5.27 Single bid
In the event of only one responsive bidder or only one bidder emerging after the evaluation process, NPCI may continue with the RFP process.

5.28 Contacting NPCI
From the time of bid opening to the time of Contract award, if any Bidder wishes to contact NPCI for seeking any clarification in any matter related to the bid, they should do so in writing by seeking such clarification/s from an authorized person. Any attempt to contact NPCI with a view to canvas for a bid or put any pressure on any official of the NPCI may entail disqualification of the concerned Bidder and/or its Bid.

Section 6 - Bid Opening

6.1 Opening of Bids

Bids will be opened in 2 stages:

Stage 1 – In the first stage the Eligibility bid i.e. Envelope 'A' and Technical Bid i.e. Envelope 'B' will be opened.

Stage 2 - In the second stage, the Commercial bids i.e. Envelope 'C' will be opened.

6.2 Opening of Eligibility and Technical Bids

NPCI will open Technical bids (Envelope 'A') and Technical bid (Envelope 'B')in presence of Bidders' representative(s) who choose to be present on the date, time and address mentioned in Section 1 or as amended by NPCI from time to time.

The representatives of the Bidders have to produce an authorization letter from the Bidder/ Identity Card to represent them at the time of opening of the bids. Only one representative will be allowed to represent each Bidder. In case the Bidder's representatives are not present at the time of opening of bids, the bids will still be opened at the scheduled time at the sole discretion of NPCI.

The bidder's representatives who are present shall sign the register evidencing their attendance. In the event of the specified date of bid opening being declared a holiday for NPCI, the bids shall be opened at the appointed time and place on next working day.

6.3 Opening of Envelope C - Commercial Bids

Only those Bids that are technically qualified will be eligible for opening of commercial bids i.e. Envelope "C" and such bidders will be intimated the date, time and address for opening of Commercial Bids.

The representatives of the Bidders have to produce an authorization letter from the Bidder/ Identity Cards to represent them at the time of opening of Commercial bids. Only one representative will be allowed to represent each Bidder. In case the Bidder's representatives are not present at the time of opening of bids, the bids will still be opened at the scheduled time at the sole discretion of the NPCI.

The bidder's representatives who are present shall sign the register evidencing their attendance. In the event of the specified date of bid opening being declared a holiday for NPCI, the bids shall be opened at the appointed time and place on next working day.

Section 7 - Bid Evaluation

7.1 Preliminary Examination of Eligibility Bids

NPCI will examine the bids to determine whether they are complete; whether required information have been provided as underlined in the bid document; whether the documents have been properly signed and whether bids are generally in order.

Eligibility and compliance to all the forms and Annexure would be the first level of evaluation. Only those Bids which comply to the eligibility criteria will be taken up for further technical evaluation.

NPCI may waive any minor informality, non-conformity or irregularity in a bid that does not constitute a material deviation provided such waiver does not prejudice or affect the relative ranking of any Bidder.

If a Bid is not substantially responsive, it will be rejected by NPCI and may not subsequently be made responsive by the Bidder by correction of the nonconformity. NPCI's determination of bid responsiveness will be based on the content of the bid itself. NPCI may interact with the Customer references submitted by Bidder, if required.

7.2 Examination of Technical Bids

The Technical Evaluation will be based on the following broad parameters:

a. Compliance to Technical Specifications as specified in the RFP.
b. NPCI reserves the right to call for presentation and discussions on the approach of execution of project etc., from the short-listed Bidders based on the technical bids submitted by them to make an evaluation. Such presentations and minutes of meetings will become part of the technical bid.
c. Review of written reply, if any, submitted in response to the clarification sought by NPCI, if any.
d. Submission of duly signed compliance statement as stipulated in Annexures. Details / Brochures containing details about the proposed solution are to be enclosed.
e. To assist in the examination, evaluation and comparison of bids NPCI may, at its discretion, ask any or all the Bidders for clarification and response shall be in writing and no change in the price or substance of the bid shall be sought, offered or permitted.
f. NPCI may interact with the Customer references submitted by bidder, if required. To assist in the examination, evaluation and comparison of bids NPCI may, at its discretion, ask any or all the Bidders for clarification and response shall be in writing and no change in the price or substance of the bid shall be sought, offered or permitted.

NPCI reserves the right to shortlist bidders based on technical evaluation criteria.

7.3 Evaluation of Commercial Bids:

Commercial bids of only the technically qualified short-listed bidders will be opened. Arithmetic errors in the Bids submitted shall be treated as follows:

- Where there is a discrepancy between the amounts in figures and in words, the amount in words shall govern;
- Where there is a discrepancy between the unit rate and the line item total resulting from multiplying the unit rate by the quantity, the unit rate will govern unless, in the opinion of NPCI, there is obviously a gross error such as a misplacement of a decimal point, in which case the line item total will govern; and
- Where there is a discrepancy between the amount mentioned in the bid and the line item total present in the Commercial Bid, the amount obtained on totalling the line items in the Commercial Bid will govern.

7.4 Successful Evaluated bidder:

After completing internal approval process, Bidder whose bid price is the lowest will be declared as successful evaluated bidder, who will be called L1 Bidder. NPCI reserves the right to place the Order with the L2 bidder, in case the L1 bidder refuses to accept the Order or otherwise gets disqualified as per the terms of the RFP, provided the L2 bidder matches the price quoted by the L1 bidder.

Section 8 - Terms and Conditions

8.1 Notification of Award / Purchase Order

After selection of the L1 bidder, as given in Clause 7.4, and after obtaining internal approvals and prior to expiration of the period of Bid validity, NPCI will send Notification of Award / Purchase Order to the selected Bidder.

Once the selected Bidder accepts the Notification of Award the selected Bidder shall furnish the Performance Bank Guarantee to NPCI.

8.2 Term of the Order

The term of the Notification of Award/Purchase Order shall be for a period of **3 years** wherein the price of the specified Web Application Firewall in the RFP would be at a fixed rate and the subsequent purchase orders with varying quantities will be issued as when requirement arises.

8.3 Acceptance Procedure

- Within 5 days of receipt of Notification of Award/Purchase Order the successful Bidder shall send the acceptance.
- Failure of the successful Bidder to comply with the above requirements shall constitute sufficient grounds for the annulment of the award

8.4 Performance Bank Guarantee

The Successful bidder shall, within 14 working days of receipt of Purchase Order, submit a Performance Bank Guarantee (PBG) equal to 10% of total value of the Purchase order (exclusive of taxes), valid for 3 years, with a claim period of 12 (twelve) months from the date of expiry of the validity period of the Bank Guarantee (BG), as per statutory provisions in force. In case the successful bidder is not in a position to submit the PBG for any reason, the successful bidder has to submit a Demand Draft drawn in favour of NPCI for equivalent amount or electronically transfer equivalent amount for credit in NPCI's account. Details of the NPCI's bank account will be furnished on request.

8.5 Taxes and Duties

All taxes deductible at source, if any, at the time of release of payments, shall be deducted at as per then prevailing rates.

Prices shall be exclusive of all taxes, duties, charges and levies of State or Central Governments as applicable. Octroi, if any, shall be reimbursed to Bidder by NPCI at actual on production of original receipt.

The bidder shall meet the requirements of applicable Goods & Services Tax (GST).

8.6 Key Deliverables:

The successful Bidder to provide the requirement of hardware, softwares and licenses as per the technical features and scope asked in the RFP.

TECHNICAL SCORING MATRIX		
Sl No	**Description**	**Score**
Technical Evaluation Part – A		30
1	Technical Requirements compliance	
2	Clarity of requirements specified in RFP	
RFP Presentation Part – B **OEM Evaluation Matrix**		10
1	Customer BFSI reference in India Size of the deployment in terms of infrastructure	

2	Faster delivery and installation	
Proposed Solution Part – C		
1	Architecture and solution Design	
2	Bidder credentials, Experience and past performance on similar contracts.	30
3	Comprehensiveness of the documents & Project Management Plan	
4	Clarity thought of delivery	
RFP Presentation Part – D		
1	RFP presentation	
2	Existing Customer reference site	30
3	Delivery of similar engagement with BFSI and backend support	
4	Q and A	
	Total Score of Part - A, B, C and D	**100**

8.7 Delivery schedule and location

The detailed activities to be completed in each phase of the project are expected below along with the timelines.

S.No.	Activity	Time Period for Completion
1	Delivery	The Hardware and software shall be delivered within 4 weeks from the date of acceptance of the Purchase Order.
2	Installation	The hardware and software Installation should be completed within 6 weeks of delivery of the hardware and software.
3	Trainings	All the trainings to be completed within 1 week from the date of request for training of NPCI officials and vendor resource based in NPCI.

8.8 Delivery Address:

Data Center – Chennai
NPCI c/o Reliance Communications Ltd.,
Reliance IDC,
1st & 6th floor Reliance House, No.6,
Haddows Road,
Nungambakkam, Chennai-600006
Kalpanarani - 9600457316

Data Center – Hyderabad
NPCI, - C/o Reliance Communications Ltd.,
Plot No 20, Survey No 64,
Opp. Mahindra Satyam,
Hitec City Layout,
Madhapur, R.R. Dist.- Hyderabad - 500 019.
Ravi Krishna - 9177733099

8.9 Incentivizing the Service Providers

a. Delivery of hardware / software / services – in case of delivery of the deliverables earlier than the stipulated delivery schedule as per the Purchase Order - 0.25% per week, for every week of early delivery, with a maximum of 2.5%, of the Order value of the respective component, i.e. hardware / software / services, as the case may be, provided the saving in delivery timeline / early delivery is not less than 20% of the prescribed delivery schedule, otherwise incentive will not be applicable. Vendors will not be eligible for any incentive if delivery happens as per the terms of the PO.

b. Incentive will not be applicable in case the original delivery schedule is extended for any reason

c. Liquidated damages will continue to be levied for delays in delivery as per the terms of the PO, if the delays are attributable to the vendors.

(i) Installation / Implementation – in case of installation of hardware/software/services before the project time line defined in the Purchase Order – 0.25% per week, for every week of early installation, with a maximum of 1%, of the Order value of the respective component, i.e. hardware / software / services, as the case may be, provided the saving in installation/ implementation timeline / early installation / implementation is not less than 20% of the prescribed installation / implementation schedule, otherwise incentive will not be applicable.

(ii) Vendors will not be eligible for any incentive if installation happens as per the terms of the PO.

8.10 Penalty for default in delivery & Installation

If the successful bidder does not deliver and install the solution as per the aforementioned schedule (Clause 8.7), or such authorized extension of delivery & installation period as may be permitted in writing by NPCI, NPCI shall impose a penalty as given below:

- Non Delivery of above at NPCI - at the rate of 0.5% of the total Purchase Order value for each week's delay beyond the stipulated delivery period subject to a maximum of 5%
- In case the delay exceeds 10 days beyond the stipulated delivery period of RFP, NPCI reserves the right to cancel the order without prejudice to other remedies available to NPCI
- Without any prejudice to NPCI's other rights under the Applicable Law, NPCI may recover the liquidated damages, if any, accruing to NPCI, as above, from any amount payable to the supplier, as per the Agreement.
- If the delay in delivery is for reason attributable to NPCI, NPCI may consider granting waiver for such delay.

8.11 Warranties and Support

- Bidder shall implement all software updates, new releases & version upgrades on the supplied components during the warranty period. Bidder should update and maintain all supplied components to correctly reflect actual state of the setup at any point in time during the warranty period
- All goods shall have the comprehensive warranty of **12 months** from the date of installation of Goods.
- The successful bidder(s) shall provide comprehensive on-site warranty for 1 year for Solution with back to back arrangements with the respective OEM from the date of acceptance of hardware / software.
- The deliverable(s) should not have been declared End of Sale as on the date of submission of the bid and on the date of delivery.
- The successful bidder(s) should ensure that the equipment proposed in this RFP, should not be declared as End of Life (EOL) or End of Support (EOS) by the OEM during the term of the Contract.

- If the deliverable(s) is declared End of Life (EOL) or End of Support anytime during the contract period, the successful bidder shall forthwith replace the equipment at no additional cost to NPCI.
- Bidder shall also update necessary OS, Patches and should support the hardware and the software for the period of three years from the date of acceptance of the entire system.
- The upgrades, new releases (Minor/major) versions, bug fixes etc. for the hardware and system software will be supplied to NPCI at no extra cost, with the necessary documentation during contract period.

8.12 Post-warranty Hardware Maintenance /AMC

- The successful bidder shall provide comprehensive on-site maintenance (AMC) of the solution with back to back support with the OEM, for a period of 2 years, after expiry of the warranty period of 1 year.
- Bidder shall provide and install patches/ updates/ version upgrades of all software provided under this contract at no extra cost to NPCI during Warranty and AMC period.
- Bidder shall provide and install patches/ updates/ version upgrades of all software provided under this contract at no extra cost to NPCI during Warranty and AMC period
- Bidder guarantees the whole of the Goods against any defects or failure, which arise due to faulty materials, workmanship or design (except materials or design furnished by NPCI).If during the Warranty Period any Goods/software are found to be damaged or defective or not acceptable, they shall promptly be replaced or rectified /re-furnished or rendered by Bidder at its own cost (including the cost of dismantling and reinstallation) on the request of NPCI and if removed from the Site for such purpose, Bidder has to provide standby Goods till the original Goods are repaired or replaced / re-furnished, rendered. All goods shall be removed and re-delivered to NPCI by Bidder at its own cost.
- Bidder shall have to submit Performance Bank Guarantee during the Warranty period equivalent to 10% of the PO value valid for period of three years

8.13 Service Level Agreement (SLA) Requirements:

The SLA specifies the expected levels of service to be provided by the Bidder to NPCI. This expected level is also called the baseline. Any degradation in the performance of the solution and services is subject to levying penalties.

Payments to the Bidder are linked to the compliance with the SLA metrics. During the contract period, it is envisaged that there could be changes to the SLAs, in terms of addition, alteration or deletion of certain parameters, based on mutual consent of both the parties i.e. NPCI and Bidder.

The Bidder shall monitor and maintain the stated service levels to provide quality service. Bidder to use automated tools to provide the SLA Reports. Bidder to provide access to NPCI or its designated personnel to the tools used for SLA monitoring.

Definitions

1. "Availability" means the time for which the services and facilities are available for conducting operations on the AIC system including application and associated infrastructure. Availability is defined as (%) = (Operation Hours –Downtime) * 100%
   (Operation Hours)
2. The business hours are 24*7 on any calendar day the NPCI is operational.
3. All the infrastructure of Data Center, Disaster Recovery site, Offices/Branches will be supported on 24x7 basis.
4. The "Operation Hours" for a given time frame are calculated after deducting the planned downtime from "Operation Hours". The Operation Hours will be taken on 24x7 basis, for the purpose of meeting the Service Level requirements i.e. availability and performance measurements both.

5. "Downtime" is the actual duration for which the system was not able to service NPCI or the Clients of NPCI, due to System or Infrastructure failure as defined by NPCI and agreed by the Bidder.
6. "Scheduled Maintenance Time" shall mean the time that the System is not in service due to a scheduled activity as defined in this SLA. The scheduled maintenance time would not be during business hours. Further, scheduled maintenance time is planned downtime with the prior permission of NPCI
7. "Incident" refers to any event / abnormalities in the functioning of any of IT Equipment / Services that may lead to disruption in normal operations of the Data Centre, System or Application services.

Interpretation & General Instructions

1. Typical Resolution time will be applicable if systems are not available to the NPCI's users.
2. The SLA parameters shall be monitored on a monthly basis as per the individual SLA parameter requirements. The Bidder is expected to provide the following service levels. In case the service levels defined in the tables below cannot be achieved, it shall result in a breach of contract and invoke the penalty clause.
3. A Service Level violation will occur if the Bidder fails to meet Minimum Service Levels on a monthly basis for a particular Service Level.
4. Quarterly SLAs would be analyzed. However, there would be month wise SLAs and all SLA targets have to be met on a monthly basis.
5. Overall Availability and Performance Measurements will be on a quarterly basis for the purpose of Service Level reporting. Month wise "Availability and Performance Report" will be provided by the Bidder for every quarter in the NPCI suggested format and a review shall be conducted based on this report. Availability and Performance Report provided to NPCI shall contain the summary of all incidents reported and associated performance measurement for that period.
6. The primary intent of Penalties is to ensure that the system performs in accordance with the defined service levels. Penalties are not meant to be punitive or, conversely, a vehicle for cutting fees.

Severity Levels

Severity Definition during Live operations due to Infrastructure/Functional issues of the proposed solution, the SLA's will be applicable post go-live of WAF Solution at DC, DRS and other NPCI Offices Description: Time taken to resolve the reported problem Severity is defined as:

Level	Function/Technologies
Severity 1	Such class of errors will include problems, which prevent users from making operational use of solution. Security Incidents like device unavailability due to any issue, hardware failure, software corruption etc. No work-around or manual process available Financial impact on NPCI Infrastructure related to providing solution to the NPCI users comprising of but not limited to the following: Proposed Solution Tools / Application Servers Proposed Solution Database Servers / Appliance Network components, if any proposed by the bidder
Severity 2	Any incident which is not classified as "Severity 1" for which an acceptable workaround has been provided by the Bidder or; Any problem due to which the Severity 2 infrastructure of the proposed solution is not available to the NPCI users or does not perform according to the defined performance and query processing parameters required as per the RFP or; Users face severe functional restrictions in the application irrespective of the cause. Key business infrastructure, systems and support services comprising of but not limited to the following: a. WAF solution Test & Development and Training Infrastructure and Application b. Infrastructure for providing access of dashboards, scorecards, etc.
Severity 3	Any incident which is not classified as "Severity 2" for which an acceptable workaround has been provided by the Bidder; Moderate functional restrictions in the application irrespective of the cause. Has a convenient and readily available

	workaround. No impact on processing of normal business activities Equipment/system/Applications issues and has no impact on the normal operations/day-today working. All other residuary proposed solution Infrastructure not defined in "Severity 1" and "Severity 2"

During the term of the contract, the bidder will maintain the equipment in perfect working order and condition and for this purpose will provide the following repairs and maintenance services

- Bidder shall complete implementation of solution as per project plan.
- Bidder shall provide technical support as well as OEM escalation support on 24X7X365 basis.
- In case of critical failures when solution software becomes unavailable due to software issues, the relevant defect should be rectified within the next business day.
- Escalation matrix shall be shared with respect to categories of incidents.

8.14 Penalty on non-adherence to SLAs:

The following Resolution Service Level Agreement (SLA) would be applicable during Warranty and AMC and are applicable for critical and non-critical incidents. The reported issue would be classified as Critical or Non-Critical by NPCI only.

a) Penalty for Severity 1 Incidents: Any violation in meeting the above SLA requirements which leads to Severity 1 incident, NPCI shall impose a penalty of INR 10,000/- (Indian Rupees Ten Thousand only) for each hour of delay up to 12 hours, beyond 12 hours penalty would be INR 20,000 for each hour with a max cap of 5% of total contract value.
b) Penalty for Severity 2: Any violation in meeting the above SLA requirements which leads to Severity 2 incident, NPCI shall impose a penalty of INR 5,000/- (Indian Rupees Five Thousand only) for each hour of delay up to 12 hours, beyond 12 hours penalty would be INR 10,000 for each hour with a max cap of 5% of total contract value.
c) Penalty for Severity 3: Any violation in meeting the above SLA requirements which leads to Severity 3 incident, NPCI shall impose a penalty of INR 2,000/- (Indian Rupees Two Thousand only) per hour with a max cap of 2% of total contract value.
d) The penalty amount would be calculated and deducted from the performance bank guarantee during warranty period and from the AMC charges payable during the period of AMC.
e) Further if the number of downtime instances during a month exceeds 3 times, an additional 0.50% downtime will be reduced from uptime and the penalty will be calculated accordingly
f) If a breach occurs even after a proper policy in WAF solution is in place, a penalty of Rs. 10,000/- per event will be deducted or the loss due to the breach whichever is higher

The right to levy the penalty is in addition to and without prejudice to other rights / remedies available to the NPCI such as termination of contract, invoking performance guarantee and recovery of amount paid etc.

8.15 Prices

Price shall remain fixed for a period of **3 years** from the date of Notification of award / 1st Purchase Order. There shall be no increase in price for any reason whatsoever and therefore no request for any escalation of the cost / price shall be entertained.

8.16 Repeat Order:

NPCI reserves the right to place Purchase Orders with the selected bidder(s) for any or all of the goods and services at the agreed unit rate, i.e. the rate contract for individual categories of WAF solution during the period of **1 year** from the date of award / 1st Purchase Order.

8.17 Product Upgrades

At any time during term of the purchase order / performance of the Contract, should technological advances be introduced by the OEM/ Supplier for information technologies originally offered by the supplier in its bid and still to be delivered, the supplier shall be obliged to offer to NPCI the latest version of the available technologies having equal or better performance or functionality at the same or lesser unit prices.

During performance of the Contract, the Supplier shall offer to NPCI all new versions, releases and updates of standard software, as well as related technical support within 30 days of their availability from the OEM.

8.18 Payment Terms:

- **Hardware:** 100% hardware cost shall be paid within 30 days after delivery and submission of correct invoice along with necessary supporting documents and hardware delivery report duly signed by NPCI officials.
- **Installation:** 100% installation cost shall be paid post implementation of the solution completely and duly certified by NPCI official.
- This would also include sign off obtained from NPCI duly certified by NPCI official

Payment shall be released within 30 days after submission of correct invoice along with necessary supporting documents and successful installation report duly signed by NPCI officials.

In the event there is any discrepancy in the Invoice and/or any in case of any incorrect invoice sent to NPCI by the successful bidder; the successful bidder would be suitably informed by NPCI to send a rectified invoice. The payment to such rectified invoice shall be made within 30 working days from date of receipt of the same.

AMC:

AMC charges shall be paid quarterly in arrears after availing maintenance services after expiry of warranty period.

Payment will be released within 30 days of receipt of correct invoices along with necessary documents / certificates duly signed by authorized NPCI official.

a. The recurring AMC charges will be paid quarterly in arrears after submission of necessary invoice and submission of quarterly reports including SLA and after deduction of penalties if any.
b. For the purpose of payment, the end of the quarter will be June, Sept, Dec and March.
c. The quarterly bills for the solution should be submitted to NPCI within 10 days of the last day of the relevant quarter.
d. Invoice shall contain all details regarding GST number, PAN, etc.

8.19 Migration activities for change of location:

In case NPCI wishes to shift the devices from one place to another anywhere in the country, adequate support will be made available by the bidder by arranging field engineer for the purpose of dismantling of devices supplied by Service provider & hand-over to the concerned Bank Officials or Data Center, pre-shifting inspection, post-shifting inspection, re-installation etc. of all devices supplied by Service provider. All migration related activities to be done after Business / session hours /according to business convenience & the engineer have to be deployed as per the bank requirements. NPCI will bear all expenses for packing, shifting, insurance and other incidentals at actual. NPCI will not be responsible or liable for any losses, damages to the items of equipment's, tools and machinery while such dismantling, pre-shifting inspection, post-shifting inspection, and re-installation etc. is being carried out. Bidder shall make available adequate alternative arrangement to ensure that the system functioning is neither affected nor dislocated during the shifting process. It is the responsibility of field engineer to integrate devices delivered for a Bank or Data Center & coordinate with NPCI NOC to extend the reachability.

8.20 Confidentiality

The Bidder shall treat the details of the documents as secret and confidential. The Successful Bidder shall execute separate NDA on the lines of the draft provided in the **Annexure Z** hereof.

In the event of disclosure of Confidential Information to a third party in violation of the provisions of this Clause, the defaulting party shall use all reasonable endeavors to assist the supplying party in recovering and preventing such third party from using, selling or otherwise disseminating of such information.

The Parties' obligations under this Section shall extend to the non-publicizing of any dispute arising out of this Agreement.

The terms of this clause shall continue in full force and effect for a period of five (5) years from the date of disclosure of such Confidential Information.

In the event of termination of this Agreement, upon written request of the disclosing Party, the receiving Party shall immediately return the disclosing Party's Confidential Information, or at the disclosing Party's option destroy any remaining Confidential Information and certify that such destruction has taken place.

8.21 Indemnity

The bidder shall indemnify, protect and save NPCI and hold NPCI harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting from any act or omission or negligence or misconduct of the bidder and its employees and representatives, breach of the terms and conditions of the agreement or purchase order, false statement by the bidder, employment claims of employees of the bidder, third party claims arising due to infringement of intellectual property rights, death or personal injury attributable to acts or omission of bidder, violation of statutory and regulatory provisions including labour laws, laws related to information technology and intellectual property rights, breach of confidentiality obligations, breach of warranty.

Indemnity would be limited to court or arbitration awarded damages and shall exclude indirect, consequential and incidental damages and compensation. Bidder shall indemnify NPCI, provided NPCI promptly notifies the Bidder in writing of such claims and the Bidder shall have the right to undertake the sole defense and control of any such claim.

8.22 Bidder's Liability

The selected Bidder will be liable for all the deliverables.

The Bidder's aggregate liability in connection with obligations undertaken under the purchase order, regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actual and limited to the value of the contract/purchase order.

The Bidder's liability in case of claims against NPCI resulting from willful and gross misconduct, or gross negligence, fraud of the Bidder, its employees, contractors and subcontractors, from infringement of patents, trademarks, and copyrights or other Intellectual Property Rights or breach of confidentiality obligations shall be unlimited.

8.23 Obligations of the Bidder

Standard of Performance: The Bidder shall perform the services and carry out their obligations with all due diligence, efficiency and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices, and employ appropriate technology and safe and effective equipment materials and methods. The Bidder shall always act in respect of any matter relating to this Contract or to the services as faithful advisor to NPCI and shall at all times support and safeguard NPCI"s legitimate interests in any dealings with third parties.

Prohibition of Conflicting Activities: The Bidder shall not engage and shall cause their personnel not to engage in any business or professional activities that would come in conflict with the activities assigned to them under the contract.

8.24 Exit option and contract re-negotiation

a) NPCI reserves its right to cancel the order in the event of happening of one or more of the situations as mentioned in the "Order Cancellation" clause

b) Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, the Bidder should continue to provide the facilities to NPCI at the site.

c) Reverse transition mechanism would be activated in the event of cancellation of the contract or exit by the parties prior to expiry of the contract. The Bidder should perform a reverse transition mechanism to NPCI or its selected vendor. The reverse transition mechanism would facilitate an orderly transfer of services to NPCI or to an alternative 3rd party / vendor nominated by NPCI. Where NPCI elects to transfer the responsibility for service delivery to a number of vendors, NPCI will nominate a service provider who will be responsible for all dealings with the Bidder regarding the delivery of the reverse transition services.

d) The reverse transition services to be provided by the Bidder shall include the following:

1. The Bidder shall suitably and adequately train NPCI or its designated team for fully and effectively manning, operating the Web Application Firewall

2. Bidder shall provide adequate documentation thereof.

3. The Bidder shall jointly manage the Web Application Firewall with NPCI or designated team for a reasonable period of time

e) Knowledge Transfer: The Bidder shall provide such necessary information, documentation to NPCI or its designee, for the effective management and maintenance of the Deliverables under this contract. Bidder shall provide documentation (in English) in electronic form where available or otherwise a single hardcopy of all existing procedures, policies and programs required for supporting the Services. Such documentation will be subject to the limitations imposed by bidder's Intellectual Property Rights of this Agreement.

f) Warranties:

1. All the warranties held by or in the name of the bidder shall be assigned or transferred as-is, in the name of NPCI. The bidder shall execute any and all such documents as may be necessary in this regard.

2. The parties shall return confidential information and will sign off and acknowledge the return of such confidential information.

3. The bidder shall provide all other services as may be agreed by the parties in connection with the reverse transition services. However, in case any other services, in addition to the above are needed, the same shall be scoped and priced.

4. The bidder recognizes that considering the enormity of the assignment, the transition services listed herein are only indicative in nature and the bidder agrees to provide all assistance and services required for fully and effectively transitioning the services provided by the bidder under the scope, upon termination or expiration thereof, for any reason whatsoever.

g) The rates for availing services during reverse transition period would be the same as payable during the contract period for the respective services.

h) During which the existing Bidder would transfer all knowledge, know-how and other things necessary for NPCI or new bidder to take over and continue to manage the services. The Bidder agrees that the reverse transition mechanism and support during reverse transition will not be compromised or affected for reasons whatsoever is for cancellation.

i) NPCI shall have the sole and absolute discretion to decide whether proper reverse transition mechanism over a period of 6 months, has been complied with. In the event of the conflict not being resolved, the conflict will be resolved through Arbitration.

j) NPCI and the bidder shall together prepare the Reverse Transition Plan. However, NPCI shall have the sole decision to ascertain whether such Plan has been complied with.

k) The Bidder agrees that in the event of cancellation or exit or expiry of the contract it would extend all necessary support to NPCI or its selected vendors as would be required

8.25 Extension of Contract

The bidder shall be required to consistently execute, in a successful and professional manner, the jobs assigned under this Contract, to the satisfaction of and as decided by the NPCI up to a period of **3 years** (completion period) reckoned from the date of commencement of the services and may be extended for further period on satisfactory performance by bidder. However even in case, the bidder is not interested to extend the Contract for a further period, bidder shall be essentially required to execute the work at least for next 6 months period on the same rates and terms & conditions of the Contract. NPCI has right to alter (increase or decrease) the number of resources. NPCI has right to place repeat order to the bidder for any resources mentioned in the Contract. The contract shall be co-terminus with the Purchase orders issued unless extended by NPCI.

8.26 Order Cancellation

NPCI reserves its right to cancel the order in the event of one or more of the following situations, that are not occasioned due to reasons solely and directly attributable to NPCI alone;

i. Delay in delivery is beyond the specified period as set out in the Purchase Order before acceptance of the product; or,

ii. Serious discrepancy in the quality of service expected.

iii. If a Bidder makes any statement or encloses any form which turns out to be false, incorrect and/or misleading or information submitted by the bidder turns out to be incorrect and/or bidder conceals or suppresses material information.

In case of order cancellation, any payments made by NPCI to the Bidder for the particular service would necessarily have to be returned to NPCI with interest @ 15% per annum from the date of each such payment. Further the Bidder would also be required to compensate NPCI for any direct loss incurred by NPCI due to the cancellation of the Purchase Order and any additional expenditure to be incurred by NPCI to appoint any other Bidder. This is after repaying the original amount paid.

8.27 Termination of Contract

For Convenience: NPCI, by written notice sent to Bidder, may terminate the contract in whole or in part at any time for its convenience giving three months prior notice. The notice of termination may specify that the termination is for convenience the extent to which Bidder's performance under the contract is terminated and the date upon which such termination become effective. NPCI shall consider request of the bidder for pro-rata payment till the date of termination.

For Insolvency: NPCI at any time may terminate the contract by giving written notice to Bidder, if Bidder becomes bankrupt or insolvent. In this event, termination will be without compensation to Bidder, provided that such termination will not prejudice or affect any right of action or remedy that has accrued or will accrue thereafter to NPCI.

For Non-Performance: NPCI reserves its right to terminate the contract in the event of Bidder's repeated failures (say more than 3 occasions in a calendar year to maintain the service level prescribed by NPCI).

8.28 Effect of Termination

- The Bidder agrees that it shall not be relieved of its obligations under the reverse transition mechanism notwithstanding the termination of the assignment.
- Same terms (including payment terms) which were applicable during the term of the contract should be applicable for reverse transition services
- The Bidder agrees that after completion of the Term or upon earlier termination of the assignment the Bidder shall, if required by NPCI, continue to provide facility to NPCI at no less favorable terms than those contained in this RFP. In case NPCI wants to continue with the Bidder's facility after the completion of this contract then the Bidder shall offer the same terms to NPCI.
- NPCI shall make such prorated payment for services rendered by the Bidder and accepted by NPCI at the sole discretion of NPCI in the event of termination, provided that the Bidder is in compliance with its obligations till such date. However, no payment for "costs incurred, or irrevocably committed to, up to the effective date of such termination" will be admissible. There shall be no termination compensation payable to the Bidder.
- NPCI may make payments of undisputed amounts to the Bidder for services rendered till the effective date of termination. Termination shall be without prejudice to any other rights or remedies a party may be entitled to hereunder or at law and shall not affect any accrued rights or liabilities or either party nor the coming into force or continuation in force of any provision hereof which is expressly intended to come into force or continue in force on or after such termination.
- Upon cancellation of contract/completion of period of service, the Bidder should peacefully handover the legal possession of all the assets provided and obtains discharge from NPCI. NPCI also reserves the right to assign or allot or award the contract to any third party upon cancellation of the availed services.

8.29 Force Majeure

If either party is prevented, restricted, delayed or interfered by reason of: a) Fire, explosion, cyclone, floods, droughts, earthquakes, epidemics; b) War, revolution, acts of public enemies, blockage or embargo, riots and civil commotion; c) Any law, order, proclamation, ordinance or requirements of any Government or authority or representative of any such Government, including restrictive trade practices or regulations; d) Strikes, shutdowns or labor disputes which are not instigated for the purpose of avoiding obligations herein; Or e) Any other circumstances beyond the control of the party affected; then notwithstanding anything here before contained, the party affected shall be excused from its performance to the extent such performance relates to prevention, restriction, delay or interference and provided the party so affected used its best efforts to remove such cause of non-performances, and when removed the party shall continue performance with the utmost dispatch.

Each of the parties agrees to give written notice forthwith to the other upon becoming aware of an Event of Force Majeure, the said notice to contain details of the circumstances giving rise to the Event of Force Majeure. If the Event of Force Majeure shall continue for more than twenty (20) days either party shall be entitled to terminate the Agreement at any time thereafter without notice.

Notwithstanding the provisions of the SOW, the successful bidder or NPCI shall not be liable for penalty or termination for default if and to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of Force Majeure. For purposes of this clause, "Force Majeure" means an event beyond the control of the successful bidder and not involving NPCI or the successful bidder's fault or negligence and not foreseeable. Such events may include, but not restricted to wars, revolutions, epidemics, natural disasters etc.

If force majeure situation arises, the successful bidder shall promptly notify NPCI in writing of such condition and cause thereof. Unless otherwise directed by NPCI in writing, the successful shall continue to perform its obligations under contract as far as possible.
Neither party shall have any liability to the other in respect of the termination of this Agreement as a result of an Event of Force Majeure.

8.30 Resolution of Disputes

All disputes or differences between NPCI and the bidder shall be settled amicably. If, however, the parties are not able to resolve them, the same shall be settled by arbitration in accordance with the applicable Indian Laws, and the award made in pursuance thereof shall be binding on the parties. Any appeal will be subject to the exclusive jurisdiction of courts at Mumbai.

NPCI and the Supplier shall make every effort to resolve amicably by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the Contract.

The dispute resolution mechanism to be applied shall be as follows:

1. In case of Dispute or difference arising between NPCI and the Supplier relating to any matter arising out of or connected with this agreement, such disputes or difference shall be settled in accordance with the Arbitration and Conciliation Act, 1996. Where the value of the Contract is above Rs.1.00 Crore, the arbitral tribunal shall consist of 3 arbitrators, one each to be appointed by NPCI and the Supplier. The third Arbitrator shall be chosen by mutual discussion between NPCI and the Supplier.
2. Arbitration proceedings shall be held at Mumbai, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English;
3. The decision of the majority of arbitrators shall be final and binding upon both parties. The cost and expenses of Arbitration proceedings will be paid as determined by the arbitral tribunal. However, the expenses incurred by each party in connection with the preparation, presentation, etc., of its proceedings as also the fees and expenses paid to the arbitrator appointed by such party or on its behalf shall be borne by each party itself; and
4. Where the value of the contract is Rs.1.00 Crore and below, the disputes or differences arising shall be referred to the Sole Arbitrator. The Sole Arbitrator should be appointed by mutual consent between the parties.

8.31 Compliance with Applicable Laws of India

The Bidder confirms to NPCI that it complies with all Central , State, Municipal laws and local laws and rules and regulations and shall undertake to observe, adhere to, abide by, comply with and notify NPCI about compliance with all laws in force including Information Technology Act 2000, or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and for all purposes of this Contract, and shall indemnify, keep indemnified, hold harmless, defend and protect NPCI and its officers/staff/personnel/representatives/agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from.
The Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate NPCI and its employees/officers/staff/personnel/ representatives/agents from and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from and NPCI will give notice of any such claim or demand of liability within reasonable time to the Bidder.

8.32 Legal Compliances:
The Bidder confirms to NPCI that its personnel/ employees/staff are covered under the provision of various Acts enacted for the protection and benefits of workmen /employees /staff or otherwise such as Employees State Insurance Act and Employees Provident Fund Miscellaneous Provision Act etc. and such other Acts like Profession Tax Act etc. as applicable and that Bidder is duly registered under the provisions of the said Acts and is complying with the provisions of the Acts.

The Bidder shall allow NPCI as well as regulatory authorities to verify books in so far as they relate to compliance with the provisions of these Acts and shall provide on demand by NPCI & regulatory authorities such documentary proof as may be necessary to confirm compliance in this regard. NPCI shall not be responsible in any event to the employees of Bidder for any of their outstanding claims or liability in that regard. NPCI shall not be responsible for any claim or demand made by such personnel for their dues outstanding against Bidder.

8.33 Intellectual Property Rights:
All rights, title and interest of NPCI in and to the trade names, trademark, service marks, logos, products, copy rights and other intellectual property rights shall remain the exclusive property of NPCI and Bidder shall not be entitled to use the same without the express prior written consent of NPCI. Nothing in contract including any discoveries, improvements or inventions made upon with/by the use of the Bidder or its respectively employed resources pursuant to contract shall either vest or shall be construed so that to vest any proprietary rights to the Bidder. Notwithstanding, anything contained in Contract, this clause shall survive indefinitely, even after termination of this Purchase Order.

8.34 Applicable Law and Jurisdiction
The Agreement shall be governed by and interpreted in accordance with the Indian Law. The jurisdiction and venue of any action with respect to the subject-matter of this Agreement shall be the Courts of Mumbai in India and each of the parties hereto submits itself to the exclusive jurisdiction and venue of such courts for the purpose of any such action.

8.35 Solicitation of Employees
Both the Parties should agree not to hire, solicit, or accept solicitation (either directly, indirectly, or through a third party) for their employees directly involved in this contract during the period of the contract and one year thereafter, except as the parties may agree on a case-by-case basis. The parties should agree that for the period of the contract and one year thereafter, neither party will cause or permit any of its directors or employees who have knowledge to directly or indirectly solicit of this contract for employing the key personnel working on the project contemplated in this proposal except with the written consent of the other party. The above restriction would not apply to either party for hiring such key personnel who (i) initiate discussions regarding such employment without any direct or indirect solicitation by the other party (ii) respond to any public advertisement placed by either party or its affiliates in a publication of general circulation or (iii) has been terminated by a party prior to the commencement of employment discussions with the other party.

8.36 Facilities provided by NPCI:
NPCI shall provide seats, with required facilities like internet, intranet & LAN Connectivity free of cost for official work. These facilities shall not be used for any personal use. In case of any misuse of the facilities, penalty as deemed fit shall be imposed and recovered from the pending bills of Bidder.

8.37 No damage of NPCI Property
Bidder shall ensure that there is no loss or damage to the property of NPCI while executing the Contract. In case, it is found that there is any such loss/damage due to direct negligence/non-performance of duty by any personnel, the amount of loss/damage so fixed by NPCI shall be recovered from Bidder.

8.38 Fraudulent and Corrupt Practice

"Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of the project and includes collusive practice among Bidder's (prior to or after Bid submission) designed to establish Bid prices at artificial non-competitive levels and to deprive the NPCI of the benefits of free and open competition.

"Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value, pressurizing to influence the action of a public official or a NPCI official in the process of project execution.

NPCI will reject a proposal for award if it determines that the Bidder recommended for award has engaged in corrupt or fraudulent practices in competing for, or in executing the project.

8.39 Governing Language

All correspondences and other documents pertaining to this Agreement shall be in English only.

8.40 Addresses for Notices

Following shall be address of NPCI and Bidder

NPCI address for notice purpose:

Managing Director& CEO

National Payments Corporation of India

1001A, B wing 10th Floor,

'The Capital', Bandra-Kurla Complex,

Bandra (East), Mumbai - 400 051

Supplier's address for notice purpose: (To be filled by supplier)

Section 9 - Technical Specifications

Please find mentioned below the technical specifications:

S. No	Requirements	Requirement Specification
1	**General**	
1.1	Solution should failover to standby site without compromising security policy defined or without impacting any changes at End users level	Must have
1.2	Solution must support a scale-out approach by having only to add more WAF appliances as needed.	Must Have
2	**Platform Architecture**	
2.1	Solution must be able to integrate with in house solutions like SIEM for sending alerts	Must Have
2.2	The solution must have a dedicated centralized management module/appliance.	Good to Have
2.3	Alerts and notification should be triggered on real time basis and distributed via mail on demand or in a scheduled manner in the form of PDF or CSV files	Must Have

General		Complied/Not Complied
1	Proposed WAF Solution should be in the Leaders quadrant in the Gartner Magic Quadrant for Web Application Firewalls at least once in last 2 years	Must have
2	The solution must be hardware appliance-based	Must have
3	The solution should support the following deployment modes to protect the application traffic: - Layer-2 transparent inline mode - Layer-3 Reverse Proxy mode	Must have
4	There must be minimal impact on the existing applications and the network architecture when deploying or removing the solution from the network.	Must have
5	The solution must support both Active-Passive & Active-Active deployment modes for high availability	Must have
6	Should support transparent failover between 2 devices, the failover should be transparent to other networking devices	Must have
7	Should support network based failover for session mirroring, connection mirroring and heartbeat check	Good to have
8	The solution appliances must have 4x1G Ethernet Interfaces	Must have
9	The solution appliances must have 2x10G SR Fiber Interfaces	Must Have
10	Should have dual power supply	Must Have
SSL Handling		
1	The proposed solution should SSL handling.	Must have
2	The system must be able to establish SSL session before sending any packet to backend servers	Must have
3	The system must support proxy SSL function that allow inspection of SSL encrypted traffic while clients are directly authenticated by the backend servers	Must have

4	The system must support elliptic curve cryptography (ECC)	Must have
5	The system must support SSL/TLS client certificate authentication	Must have
6	The system should support TLS v1.2 & TLS v1.3	Must have
7	Proposed solution should have the ability to granularly define the key exchange algorithm, ciphers and signing algorithm for each application service	Must have
8	The system must support SSL/TLS client certificate authentication	Must have
9	The system must store the certificate private key using a secure mechanism	Must Have
10	The system must store the certificate private key using a secure mechanism, and a passphrase	Must have
11	The system must capable of communication with the original backend application server over SSL or TLS. should have the ability to granularly define the key exchange algorithm, ciphers and signing algorithm for the SSL/TLS connection to the backend server	Must Have
12	The solution must have a SSL hardware module to support minimum 9K SSL TPS on RSA and minimum 5K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key	Must Have
Application DDOS Protection		
1	The system must be able to mitigate DoS vectors focusing on protocol weaknesses of HTTP such that: a. Slowloris b. Slow Post d. HTTP GET/POST Flood	Must Have
2	The proposed solution should protect against Ability to allow only specific HTTP Methods.	Must Have
3	The proposed solution should have the capability to proactively identify bots.	Must Have
Web Application Firewall Features		
1	The system must capable of blocking specific list of HTTP methods	Must Have
2	The system must be able to allow or disallow specific file type	Must Have
3	The system must be able to enforce specific HTTP headers and values to be present in client requests	Must Have
4	The system must support protection of Common Web Application attacks including OWASP Top 10 vulnerabilities, etc	Must Have
5	The system must be able to perform information display masking/scrubbing on requests and responses	Good to Have
6	The solution must support the positive security model approach. A positive security model states what input and behavior is allowed and everything else that deviates from the positive security model is alerted and/or blocked	Must Have
7	The solution must support the negative security model approach. A negative security model explicitly defines known attack signatures	Must Have
8	The solution must be able to block transactions with content matching known attack signatures while allowing everything else	Must Have
9	The solution must be able to support both inline and non-inline monitoring-only and active enforcement mode. In monitoring-only mode, the administrator can view alerts, attacks, server errors, and other unauthorized activity. In active enforcement mode, the solution can perform everything that is done in monitoring-only	Must Have

	mode and additionally be able to block attacks	
10	The solution must be able to execute the following actions upon detecting an attack or any other unauthorized activity: a. Ability to drop requests and responses, b. Block the TCP session, c. Block the application user, or d. Block the IP address	Must Have
11	The solution must be able to block the user or the IP address for a configurable period of time	Must Have
12	The solution must be able to send a TCP RST packet to both ends of a web connection when it is deployed in sniffing mode in the event of active enforcement deployment mode	Must Have
13	The solution must be able to protect both HTTP Web applications and SSL (HTTPS) web applications	Must Have
14	The solution must be able to decrypt SSL web traffic between clients and web servers	Must Have
15	The solution must be able to decrypt SSL web traffic that are using Diffie-Hellman key exchange protocols with the monitoring appliance deployed in transparent layer-2 mode	Must Have
16	The solution must provide the ability to comply to A+ Certification at the click of a button	Must Have
17	The solution must provide the ability to control SSL settings via a GUI based interface	Must Have
18	The solution must be able to decrypt SSL web traffic for inspection without terminating or changing the HTTPS connection	Must Have
19	The solution must provide the following features and protection: a. HTTP protocol validation b. Correlated based attack protection c. HTTP protocol attack signatures d. Cookie signing validation e. Anti-website scraping f. Whitelisting based protection g. Web worm protection h. Web application attack signatures i. Web application layer customized protection	Must Have
20	The proposed WAF should protects against various application attacks, including: a. Layer 7 DoS and DDoS b. Brute force c. Cross-site scripting (XSS) d. Cross Site Request Forgery e. SQL injection f. Form Field and Parameter Tampering and HPP tampering g. Sensitive information leakage h. Session highjacking i. Buffer overflows j. Cookie manipulation/poisoning k. Various encoding attacks l. Broken access control m. Forceful browsing n. Hidden fields manipulation o. Request smuggling p. XML bombs/DoS	Must Have
21	The solution must include a pre-configured list of comprehensive and accurate web attack signatures	Must Have

22	The solution must have a database of signatures that are designed to detect known problems and attacks on web applications	Must Have
23	The solution must be able to prevent attacks that are using Base64 encoded parameters and headers	Must Have
24	The solution must provide signature protection against known vulnerabilities in commercial infrastructure software such as Apache, IIS and so on. The content provided by the signature detection mechanism must be based on the research done by the solution vendor threat intelligence division and a combination of other resources such as Snort, CVE and so on. This set of signatures must be continuously and automatically updated	Must Have
25	The solution must allow administrators to add and modify signatures	Must Have
26	The solution must support regular expressions for the following purposes: a. Signatures definition b. Sensitive data definition c. Parameter type definition d. Host names and URL prefixes definition e. Fine tuning of parameters that are dynamically learnt from the web application profile	Must Have
27	The solution must support automatic updates to the signature database to ensure complete protection against the latest web application threats	Must Have
28	The solution must be able to detect known attacks at multiple levels. This includes network, Web server software and application-level attacks	Must Have
29	The solution's in-built correlation engine must address complex attacks that are ambiguous in nature. It must also examine multiple pieces of information at the network, protocol and application levels over time to distinguish between attacks and valid user traffic	Must Have
30	The solution must inspect and monitor all HTTP(S) data and the application level including HTTP(S) headers, form fields, and the HTTP(S) body	Must Have
31	The solution must be able to inspect HTTP requests and responses	Must Have
32	The solution must be able to identify Web Socket connections.	Must Have
33	The Solution must be able to parse and monitor JSON data over web socket protocol	Must Have
34	The solution must be able to inject HTML snippet/text in the HTTP response	Must Have
35	The solution must automatically discover HTTP traffic content type, regardless of the content-type HTTP header. With this capability, WAF should be able to parse and protect HTTP Requests with missing or wrong content-type header	Must Have
36	The solution must be able to validate encoded data in the HTTP traffic.	Must Have
37	The solution should protect against Deserialization attacks, accomplished by searching for signatures in the 'Request-Content' header	Must Have
38	The solution must be able to perform validation on all types of input, including URLs, forms, cookies, query strings, hidden fields, and parameters, HTTP methods, XML elements and SOAP actions.	Must Have
39	The solution must be capable to automatically create whitelisting/profiling of web applications.	Must Have

40	The solution profiling technology must be able to detect and protect against threats which are specific to the custom code of the web application. After the profiling/learning phase, the solution must be able to understand the structure of each protected URL.	Must Have
41	The solution must automatically build/learn the web application profiles and use them to detect deviations and various anomalies (or violations) and block attacks on the custom code of the application.	Must Have
42	The solution must be able to automatically learn the web usage and application structure and elements and expected user behaviors as soon as the system is installed.	Must Have
43	The structure and elements include URLs, directories, cookies, form fields and parameters, and HTTP methods.	Must Have
44	User behaviors include expected value length; acceptable characters per parameter field; whether the parameter value is read-only or editable by the user and whether the parameter is mandatory or optional.	Must Have
45	The solution must be able to automatically switch profile to the enforcement mode after a suitable learning period which can be defined manually by the administrator.	Must Have
46	The solution profiling learning mode must be able to recognize changes to the web application and simultaneously protect web applications at the same time.	Must Have
47	The solution must be able to learn and create profile and in parallel should protect application by blocking malicious requests using negative security model based policies.	Must Have
48	The solution must allow profiles to be manually changed and information can be added and removed to fine tune the profiles.	Must Have
49	The solution must support profiling from only a set of trusted users to learn the normal acceptable behavior and usage of the web application.	Must Have
50	The solution must allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.	Must Have
51	The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in learning mode.	Must Have
52	The solution must be able to perform profiling of web applications in an environment where there is a mixture of good and bad traffic. The solution must be able to automatically differentiate good and bad traffic when learning the profile. Bad traffic should not be learnt	Must Have
53	The solution must be able to automatically learn all the host names of the web applications being protected.	Must Have
54	The solution must be able to perform profiling of JSON. HTTP requests in the JSON format must be learnt by the WAF with the parameters and values.	Must Have
55	The solution must be able to protect web applications that include Web services (XML) content.	Must Have
56	The XML protection offered by the solution must be similar to the web application protection provided with automated profiling/learning capability.	Must Have
57	The solution must support custom security rules. Administrators should be able to define rules for the positive and negative security model and to create correlation rules with multiple	Must Have

	criteria.	
58	The solution must be able to perform virtual patching for its protected web applications.	Must Have
59	The solution must support all the following web application vulnerability assessment tools (Web application scanners) to virtually patch web application vulnerabilities: a. Cenzic b. HP Fortify WebInspect c. IBM AppScan d. Qualys e. WhiteHat	Must Have
60	The solution must address and mitigate the OWASP Top Ten web application security vulnerabilities. Describe how each of the OWASP Top Ten vulnerability is addressed by the solution.	Must Have
61	The solution must support the capability to define security policies based on the threat intelligence feeds listed previously to perform the following functions: a. Alert b. Block IP c. Block Session d. Block User	Must Have
62	The proposed WAF should be session aware and should be able to enforce and report session	Must Have
63	The solution must be able to track and monitor web application users. This user tracking mechanism must be automated, with no changes to the existing application or authentication scheme.	Must Have
64	The solution must support user tracking using both form-based and certificate-based user authentication.	Must Have
65	The solution must provide automated, real-time event alert mechanism.	Must Have
66	The solution must be able to monitor and block users when required.	Must Have
67	The solution must support masking of sensitive data in alerts.	Must Have
68	The solution must support sending of logs in CEF standard.	Must Have
69	The solution must support a flexible set of follow-up actions to be taken in the event of an alert generation. For example, if an alert is generated based on a Policy, send an email to Administrator X and Manager Y followed by sending a syslog to Destination 1 and a CEF-formatted log to Destination 2.	Must Have
70	Should support manual as well as automatic online updation of the Signatures	Must Have
71	Signature updation should be independent of the underlying firmware OS	Must Have
72	Signature updation should be not cause any downtime	Must Have
73	The proposed WAF should protect from HPP attacks	Must Have
74	The proposed WAF should support Policy Evasion Detection Engine	Must Have
75	The proposed WAF should be able to do Manipulation of invalidated input	Must Have
76	The proposed WAF should protect against Remote File Inclusion Attacks	Must Have
77	The proposed WAF should protect against requests for restricted object and file types	Must Have
78	The proposed WAF should protect unauthorized navigation	Must Have
79	The proposed WAF should protect against Directory/Path traversal	Must Have

80	The proposed WAF should protect against known worms and vulnerabilities	Must Have
81	The proposed WAF should prevent OS and web server fingerprinting	Must Have
82	The proposed WAF should conceal any HTTP error messages from users	Must Have
83	The proposed WAF should remove application error messages from pages sent to users	Must Have
84	The proposed WAF should prevent leakage of server code	Must Have
85	The proposed WAF should support Schema validation	Must Have
86	The proposed WAF should support Parser protection (XML Bombs, Recursion Attacks)	Must Have
87	The proposed WAF should support XPATH injection	Must Have
88	The proposed WAF should support RSS/Atom feed injection	Must Have
89	The proposed WAF should support XML islands	Must Have
91	The proposed WAF should be capable to trigger a script based on an event	Must Have
92	The proposed WAF should support staging of policies/attack signatures before being enforced. The staging to automatic enforcing time period should be customizable	Must Have
93	The proposed WAF should provide application-specific XML filtering and validation functions that ensure the XML input of web-based applications is properly structured. It should provide schema validation, common attacks mitigation, and XML parser denial-of-service prevention.	Must Have
94	The WAF must be able to inject a JavaScript challenge instead of the original response in order to test whether the client is a legitimate browser or a bot	Must Have
Reporting Features		
1	The system must be able to display attacks and its mitigation statistics	Must Have
2	The system must equip with a high-speed logging mechanism which can send log message in near real-time without significantly impacting system performance.	Must Have
4	The system shall have ability to identify and notify system faults and loss of performance (SNMP, syslog, e-mail, etc)	Must Have
5	The system shall have ability to customize logging	Must Have
6	The system must provide request logging that support profile by enabling configuration log entries to be reported when requests/responses are received, supports audit logging of HTTP/decrypted HTTPS requests/responses, and enables specification of a response to be issued when a specific requests/responses occur.	Good to Have
7	The system must provide response logging so that it helps in analyzing responses is especially useful when logging response-related security events, such as Data Guard or response signatures, it is also be useful in analyzing request violations, to determine whether they represent an actual attack or a false positive	Good to Have
8	The system shall have ability to generate service and system statistics. Provides dashboard displays anomaly statistics about number attacks, dropped requests, a summary of system traffic.	Good to Have
9	The system must provide high-level view of recent activity in a single screen, where you can view aggregated events (incidents) rather than individual transactions (that are displayed on the Requests screen). Incidents are suspected attacks on the web	Must Have

	application.	
10	The system shall be capable of logging security events with Syslog	Must Have
11	The system shall be capable of logging security events with SNMP as well as SNMP MIB is polled for information about any current active attacks	Must Have
12	The system must provide built in logging to 3rd party security event tracking systems such as SIEM like Arcsight or Splunk	Must Have
13	The proposed solution should have the capability to capture tcpdump for forensic analysis.	Must Have
14	The proposed solution should have the capability to create a granular logging policy per application.	Must Have
15	The proposed solution should have the capability to define a customized log format for each application.	Must Have
16	The proposed solution should have the capability to define multiple log destinations for each application	Must Have
17	The solution must provide pre-packaged reporting capabilities out-of-the-box without user intervention/further configuration: a. Alert analysis (For Application user, Known attack patterns, severity, Source IP with severity & type, URL, User with severity & type, Violation Types) b. Daily & weekly Top 10 WAF violations c. Daily Summary Blocked Connections d. Data Leakage Report e. Directory Browsing Detection Report f. List of Alerts g. PCI - WAF violations h. Sensitive Error Messages Leakage Report i. Slow HTTP/S Alerts	Must Have
18	The solution must have the functionality within the UI out-of-the-box that enables the administrator to create custom report templates based on the existing out-of-the-box reports.	Must Have
19	The solution must support automatic generation of reports based on a defined schedule.	Must Have
20	The solution must support scheduling of report generation to start only at a future date.	
Management		
1	Proposed hardware solution should have a dedicated out-of-band management port	Must Have
2	Proposed solution should have Web GUI (HTTPS) for management. The solution must allow the user to use a standard browser to access the management UI	Must Have
3	Proposed solution should have CLI (SSH) for management	Must Have
4	Proposed solution should have the capability to restrict SSH from specific IP address	Must Have
5	Proposed solution should have the capability to restrict Shell access tp specific users	Must Have
6	Proposed solution should have the capability to define an ACL for Web/CLI access	Must Have
7	Proposed solution should have the detailed Access logs for audit trail purpose	Must Have
8	The system must support Network Time Protocol (NTP) to synchronize its clock with an NTP server	Must Have
9	The entire solution must be centrally managed for day to day operations. The management server must centrally manage all the appliances.	Must Have

10	Reporting, policy creation, alerts management, web application protection configuration, etc must be managed from the management server.	Must Have
11	The proposed solution should have Role based access	Must Have
12	The solution must provide Role-Based Access Control. It should at minimum have the below user roles that facilitate separation of duties. a. Administrator b. Manager c. Auditor d. Operator e. SSL Certificate Manager f. Guest	Must Have
13	The solution must support the following authentication mechanism for accessing the solution management UI: - In-built authentication in the solution - LDAP - RADIUS	Must Have
14	The solution must support the following password management capabilities without relying on any external system: a. Password validity period in days b. Password length (minimum required number of characters in the password.) c. Whether a password must be significantly different from the last password used d. Whether a password must include capital letters, numbers, lower case letters and non-alphanumeric characters or not.	Must Have
15	The solution must be able to support the configuration of the following lockout settings from the solution management UI: a. Login failed attempts period (in minutes) in which entering an incorrect password multiple times locks an account b. Number of failed login attempts which result an account to be locked c. Lock duration in minutes	Must Have
16	The solution must support the capability of trust-based communication between the different components in the solution. i.e. Communication between solution components needs to be done using certificates.	Must Have

Section 10 - Documents forms to be put in Envelope A

Annexure A1 - Bidder's Letter for EMD

To

The Chief Executive Officer
National Payments Corporation of India,
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Subject: RFP No. NPCI/RFP/2018-19/IT/17 dated 25.02.2019 for "Request for Proposal for supply and installation of Web Application Firewall".

We have enclosed an EMD in the form of a Demand Draft No.____ issued by the branch of the _____Bank, for the sum of Rs. _____ (Rupees _____). This EMD is as required by clause 5.7 of the Instructions to Bidders of the above referred RFP.

Thanking you,

Yours faithfully,

(Signature of the Bidder)
Printed Name:
Designation:
Seal:
Date:
Business Address:

Annexure A2 - Bid Security (Bank Guarantee)

_____
[Bank's Name, and Address of Issuing Branch or Office]

National Payments Corporation of India: _____

Date: _____

BID GUARANTEE No.: _____

We have been informed that_____ (hereinafter called "the Bidder") has submitted to you its bid dated (hereinafter called "the Bid") for the execution of _____under RFP No.

Furthermore, we understand that, according to your conditions, bids must be supported by a bank guarantee.

At the request of the Bidder, we _____ hereby irrevocably undertake to pay you without any demur or protest, any sum or sums not exceeding in total an amount of Rs._____/-(Rupees _____ only) upon receipt by us of your first demand in writing accompanied by a written statement stating that the Bidder is in breach of its obligation(s) under the bid conditions, because the Bidder:

(a) Has withdrawn its Bid during the period of bid validity specified by the Bidder in the Form of Bid; or

(b) having been notified of the acceptance of its Bid by NPCI during the period of bid validity, (i) fails or refuses to execute the Contract Form; or (ii) fails or refuses to furnish the performance security, if required, in accordance with the Instructions to Bidders.

This guarantee will expire:

(a) If the Bidder is the successful bidder, upon our receipt of copies of the contract signed by the Bidder and the performance security issued to you upon the instruction of the Bidder; or

(b) if the Bidder is not the successful bidder, upon the earlier of (i) our receipt of a copy of your notification to the Bidder of the name of the successful bidder; or (ii) twelve months after the expiration of the Bidder's Bid.

Consequently, any demand for payment under this guarantee must be received by us at the Office on or before that date.

_____
[Signature]

Annexure A3 - Bid Security (Performance Bank Guarantee)

(BANK GUARANTEE)

Date
Beneficiary: NATIONAL PAYMENTS CORPORATION OF INDIA
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Performance Bank Guarantee No:
We have been informed that----------(hereinafter called "the Supplier") has received the purchase order no. "----------" dated ---------- issued by National Payments Corporation of India (NPCI), for ---------- (hereinafter called "the Purchase Order").

Furthermore, we understand that, according to the conditions of the Purchase order, a Performance Bank Guarantee is required to be submitted by the Supplier to NPCI.
At the request of the Supplier, We ----------(name of the Bank , the details of its incorporation) having its registered office at ---------- ---------- and, for the purposes of this Guarantee and place where claims are payable, acting through its ---- branch presently situated at ---------- (hereinafter referred to as "Bank" which term shall mean and include, unless repugnant to the context or meaning thereof, its successors and permitted assigns),hereby irrevocably undertake to pay you without any demur or objection any sum(s) not exceeding in total an amount of Rs.---------- (in figures) (Rupees---------(in words)------- only) upon receipt by us of your first demand in writing declaring the Supplier to be in default under the purchase order, without caveat or argument, or your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

Please note that you may, if you so require, independently seek confirmation with –(Bank Name & Issuing branch address)----------, that this Bank Guarantee has been duly and validly issued.

Notwithstanding anything contained in the foregoing:
The liability of ---------- (Bank), under this Bank Guarantee is restricted to a maximum total amount of Rs. ---------- (Amount in figures and words).
This bank guarantee is valid upto ----------.
The liability of ---------- (Bank), under this Bank Guarantee is finally discharged if no claim is made on behalf of NPCI within twelve months from the date of the expiry of the validity period of this Bank Guarantee.
Our liability pursuant to this Bank Guarantee is conditional upon the receipt of a valid and duly executed written claim or demand, by ---------- (Bank)---------- -------- (Address), delivered by hand, courier or registered post, or by fax prior to close of banking business hours on ---------- (date should be one year from the date of expiry of guarantee) failing which all rights under this Bank Guarantee shall be forfeited and ---------- (Bank), shall stand absolutely and unequivocally discharged of all of its obligations hereunder.

This Bank Guarantee shall be governed by and construed in accordance with the laws of India and competent courts in the city of Mumbai shall have exclusive jurisdiction.

Kindly return the original of this Bank Guarantee to ---------- --------- (Bank & Its Address), upon (a) its discharge by payment of claims aggregating to Rs. -------- (Amount in figures & words); (b) Fulfillment of the purpose for which this Bank Guarantee was issued; or (c) Claim Expiry Date (date should be one year from the date of expiry of this Bank Guarantee).
All claims under this Bank Guarantee will be payable at ---------- ---------- (Bank & Its Address).

{Signature of the Authorized representatives of the Bank}

Annexure B - Bid Offer Form (without Price)

(Bidder's Letter Head)

OFFER LETTER

Date:

To

The Chief Executive Officer
National Payments Corporation of India
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Dear Sir,

Subject: RFP No. NPCI/RFP/2018-19/IT/17 dated 25.02.2019 for "Request for Proposal for supply and installation of Web Application Firewall".

We have examined the above referred RFP document. As per the terms and conditions specified in the RFP document, and in accordance with the schedule of prices indicated in the commercial bid and made part of this offer.
We acknowledge having received the following addenda / corrigenda to the RFP document.

Addendum No. / Corrigendum No.	Dated

While submitting this bid, we certify that:

1. Prices have been quoted in INR.
2. The prices in the bid have not been disclosed and will not be disclosed to any other bidder of this RFP.
3. We have not induced nor attempted to induce any other bidder to submit or not submit a bid for restricting competition.
4. We agree that the rates / quotes, terms and conditions furnished in this RFP are for NPCI and its Associates.

If our offer is accepted, we undertake, to start the assignment under the scope immediately after receipt of your order. We have taken note of Penalty clauses in the RFP and agree to abide by the same. We also note that NPCI reserves the right to cancel the order and order cancellation clause as per terms and condition would be applicable. We understand that for delays not attributable to us or on account of uncontrollable circumstances, penalties will not be levied and that the decision of NPCI will be final and binding on us.

We agree to abide by this offer till 180 days from the last date stipulated by NPCI for submission of bid, and our offer shall remain binding upon us and may be accepted by NPCI any time before the expiry of that period.

Until a formal contract is prepared and executed with the selected bidder, this offer will be binding on us. We also certify that the information/data/particulars furnished in our bid are factually

correct. We also accept that in the event of any information / data / particulars are found to be incorrect, NPCI will have the right to disqualify /blacklist us and forfeit bid security.

We undertake to comply with the terms and conditions of the bid document. We understand that NPCI may reject any or all of the offers without assigning any reason whatsoever.

As security (EMD) for the due performance and observance of the undertaking and obligation of the bid we submit herewith Demand Draft bearing no. _____dated _____ drawn in favor of "National Payments Corporation of India" or Bank Guarantee valid for ____days for an amount of Rs._____ (Rs. _____ only) payable at Mumbai.

Yours sincerely,

Authorized Signature [In full and initials]:

Name and Title of Signatory:

Name of Company/Firm:

Address

Annexure C - Bidder Information

Details of the Bidder				
1	Name of the Bidder (Prime)			
2	Address of the Bidder			
3	Constitution of the Company (Public Ltd/ Pvt Ltd)			
4	Details of Incorporation of the Company.	Date:		
		Ref#		
5	Permanent Account Number (PAN)			
6	Goods & Services Tax (GST) Registration Numbers			
7	Name & Designation of the contact person to whom all references shall be made regarding this tender			
8	Telephone No. (Cell # and Landline # with STD Code)			
9	E-Mail of the contact person:			
10	Fax No. (with STD Code)			
11	Website			
Financial Details (as per audited Balance Sheets) (in Cr)				
12	Year	2015-16	2016-17	2017-18
13	Net worth			
14	Turn Over			
15	PAT			

Annexure D - Declaration for Clean Track Record

To

The Chief Executive Officer
National Payments Corporation of India
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Sir,

I have carefully gone through the Terms & Conditions contained in the RFP document for selection of vendor for **Request for Proposal for supply and installation of Web Application Firewall - RFP No. NPCI/RFP/2018-19/IT/17 dated 25.02.2019.**I hereby declare that my company has not been debarred/black listed by any Government / Semi Government / Private organizations in India / abroad. I further certify that I am competent officer and duly authorized by my company to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address:

Annexure E - Declaration for Acceptance of RFP Terms and Conditions

To

The Chief Executive Officer
National Payments Corporation of India
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Dear Sir,

I have carefully gone through the Terms & Conditions contained in the RFP document for selection of vendor for **Request for Proposal for supply and installation of Web Application Firewall - RFP No. NPCI/RFP/2018-19/IT/17 dated 25.02.2019.** I declare that all the provisions of this RFP/Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address:

Annexure F - Declaration for Acceptance of Scope of Work

To

The Chief Executive Officer
National Payments Corporation of India
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Sir,

I have carefully gone through the Scope of Work contained in the RFP document for selection of vendor for **Request for Proposal for supply and installation of Web Application Firewall - RFP No. NPCI/RFP/2018-19/IT/17 dated 25.02.2019.** I declare that all the provisions of this RFP / Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address:

Annexure G - Format Power of Attorney

(On Stamp paper of relevant value)

Know all men by the present, we _____ (name of the company and address of the registered office) do hereby appoint and authorize _____ (full name and residential address) who is presently employed with us holding the position of _____ as our attorney, to do in our name and on our behalf, deed and things necessary in connection with or incidental to our proposal for **Request for Proposal for supply and installation of Web Application Firewall - RFP No. NPCI/RFP/2018-19/IT/17 dated 25.02.2019** in response to the RFP by NPCI, including signing and submission of all the documents and providing information/responses to NPCI in all the matter in connection with our bid. We hereby agree to ratify all deeds and things lawfully done by our said attorney pursuant to this Power of Attorney and that all deeds and things done by our aforesaid attorney shall always be deemed to have been done by us.

Dated this _____ day of _____ 2019.
For _____.

(Signature)

(Name Designation and Address)

Accepted

(Signature)
(Name Designation)
Date:
Business Address:

Annexure H - Eligibility Criteria Compliance

Sr.No	Eligibility Criteria	Compliance Yes/No	Documentary proof to be attached
1	The bidder is a Company registered under the Companies Act/ Partnership / LLP at least since last three years. a. In case the bidder is the result of a merger / acquisition, at least one of the merging companies should have been in operation for at least 3 years as on date of submission of the bid. b. In case the bidder is the result of a demerger / hiving off, at least one of the demerged company or resulting company should have been in operation for at least 3 years as on the date of submission of bid.		Documentary Proof should be submitted
2	The bidder should have reported minimum annual turnover of Rs. 10 Crores as per audited financial statements in each of the last three financial years (i.e.2015-2016, 2016-2017 & 2017-2018) and should have reported profits (profit after tax) as per audited financial statements in at least two of last three financial years (i.e., 2015-2016, 2016-2017 & 2017-2018). In case audited financial statements for 2017-2018 are not ready, then management certified financial statement shall be considered for 2017-2018, however, this exception is not available in case of previous financial years. In case of a JV / Consortium / Strategic partnership, the bidder should have reported profits as per above criteria. a. In case the bidder is the result of a merger / acquisition, due consideration shall be given to the past financial results of the merging entity for the purpose of determining the net worth, minimum annual turnover and profit after tax for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 3 years. For this purpose, the decision of NPCI will be treated as final and no further correspondence will be entertained on this. b. In case the bidder is the result of a demerger / hiving off, due consideration shall be given to the past financial results of the demerged company for the purpose of determining the net worth, minimum annual turnover and profit after tax for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 3 years. For this purpose, the decision of NPCI will be treated as final and no further correspondence will be entertained on this.		Standalone financial Audited balance sheets & Profit /loss statement, Statutory Auditor's Report, Notes to Accounts and Schedules forming part of accounts to be submitted.
3	The bidder should be authorized to quote for the OEM products and support. Further, the bidder shall submit the declaration stating that bidder will not remain associated with this RFP in any other capacity as a part of distribution channel provided such bidder has become eligible for commercial evaluation as per		• Declaration from OEM (OEM to provide self-declaration to the effect on company letter head)

	this RFP.		• Declaration from the bidder stating that bidder will not remain associated with this RFP
4	The Bidder should not be currently blacklisted by any bank / institution in India or abroad.		Self-Declaration as per Annexure D

Annexure I - OEM / Manufacturer's Authorization Letter

[The Bidder shall require the Manufacturer to fill in this Form in accordance with the instructions indicated. This letter of authorization should be on the letterhead of the Manufacturer and should be signed by a person with the proper authority to sign documents that are binding on the Manufacturer. The Bidder shall include it in its bid]

Date:

To:

WHEREAS

We_____, are official manufacturers/OEM vendors of_____. We_____ do hereby authorize M/S_____ to submit a bid the purpose of which is to provide the following Goods, manufactured by us _____, and to subsequently negotiate and sign the Contract.

We hereby extend our full guarantee and warranty, with respect to the Goods offered by the above firm.

Signed by the Manufacturer/OEM Vendor:

Name:

Title:

Seal:

Dated on _____ day of _____, _____

Section 11 - Documents to be put in Envelope 'B'

Annexure K - Technical Compliance

S. No	Requirements	Requirement Specification	Complied (Yes/No)
1	**General**		
1.1	Solution should failover to standby site without compromising security policy defined or without impacting any changes at End users level	Must have	
1.2	Solution must support a scale-out approach by having only to add more WAF appliances as needed.	Must Have	
2	**Platform Architecture**		
2.1	Solution must be able to integrate with in house solutions like SIEM for sending alerts	Must Have	
2.2	The solution must have a dedicated centralized management module/appliance.	Good to Have	
2.3	Alerts and notification should be triggered on real time basis and distributed via mail on demand or in a scheduled manner in the form of PDF or CSV files	Must Have	

	General	Complied/Not Complied	Complied (Yes/No)
1	Proposed WAF Solution should be in the Leaders quadrant in the Gartner Magic Quadrant for Web Application Firewalls at least once in last 2 years	Must have	
2	The solution must be hardware appliance-based	Must have	
3	The solution should support the following deployment modes to protect the application traffic: - Layer-2 transparent inline mode - Layer-3 Reverse Proxy mode	Must have	
4	There must be minimal impact on the existing applications and the network architecture when deploying or removing the solution from the network.	Must have	
5	The solution must support both Active-Passive & Active-Active deployment modes for high availability	Must have	
6	Should support transparent failover between 2 devices, the failover should be transparent to other networking devices	Must have	
7	Should support network based failover for session mirroring, connection mirroring and heartbeat check	Good to have	
8	The solution appliances must have 4x1G Ethernet Interfaces	Must have	
9	The solution appliances must have 2x10G SR Fiber Interfaces	Must Have	
10	Should have dual power supply	Must Have	

SSL Handling			
1	The proposed solution should SSL handling.	Must have	
2	The system must be able to establish SSL session before sending any packet to backend servers	Must have	
3	The system must support proxy SSL function that allow inspection of SSL encrypted traffic while clients are directly authenticated by the backend servers	Must have	
4	The system must support elliptic curve cryptography (ECC)	Must have	
5	The system must support SSL/TLS client certificate authentication	Must have	
6	The system should support TLS v1.2 & TLS v1.3	Must have	
7	Proposed solution should have the ability to granularly define the key exchange algorithm, ciphers and signing algorithm for each application service	Must have	
8	The system must support SSL/TLS client certificate authentication	Must have	
9	The system must store the certificate private key using a secure mechanism	Must Have	
10	The system must store the certificate private key using a secure mechanism, and a passphrase	Must have	
11	The system must capable of communication with the original backend application server over SSL or TLS. should have the ability to granularly define the key exchange algorithm, ciphers and signing algorithm for the SSL/TLS connection to the backend server	Must Have	
12	The solution must have a SSL hardware module to support minimum 9K SSL TPS on RSA and minimum 5K on ECC with 2K Keys. SSL TPS means new SSL handshakes per second without reuse of session key	Must Have	
Application DDOS Protection			
1	The system must be able to mitigate DoS vectors focusing on protocol weaknesses of HTTP such that: a. Slowloris b. Slow Post d. HTTP GET/POST Flood	Must Have	
2	The proposed solution should protect against Ability to allow only specific HTTP Methods.	Must Have	
3	The proposed solution should have the capability to proactively identify bots.	Must Have	
Web Application Firewall Features			
1	The system must capable of blocking specific list of HTTP methods	Must Have	
2	The system must be able to allow or disallow specific file type	Must Have	
3	The system must be able to enforce specific HTTP headers and values to be present in client requests	Must Have	
4	The system must support protection of Common Web Application attacks including OWASP Top 10 vulnerabilities, etc	Must Have	
5	The system must be able to perform information display masking/scrubbing on requests and responses	Good to Have	

6	The solution must support the positive security model approach. A positive security model states what input and behavior is allowed and everything else that deviates from the positive security model is alerted and/or blocked	Must Have	
7	The solution must support the negative security model approach. A negative security model explicitly defines known attack signatures	Must Have	
8	The solution must be able to block transactions with content matching known attack signatures while allowing everything else	Must Have	
9	The solution must be able to support both inline and non-inline monitoring-only and active enforcement mode. In monitoring-only mode, the administrator can view alerts, attacks, server errors, and other unauthorized activity. In active enforcement mode, the solution can perform everything that is done in monitoring-only mode and additionally be able to block attacks	Must Have	
10	The solution must be able to execute the following actions upon detecting an attack or any other unauthorized activity: a. Ability to drop requests and responses, b. Block the TCP session, c. Block the application user, or d. Block the IP address	Must Have	
11	The solution must be able to block the user or the IP address for a configurable period of time	Must Have	
12	The solution must be able to send a TCP RST packet to both ends of a web connection when it is deployed in sniffing mode in the event of active enforcement deployment mode	Must Have	
13	The solution must be able to protect both HTTP Web applications and SSL (HTTPS) web applications	Must Have	
14	The solution must be able to decrypt SSL web traffic between clients and web servers	Must Have	
15	The solution must be able to decrypt SSL web traffic that are using Diffie-Hellman key exchange protocols with the monitoring appliance deployed in transparent layer-2 mode	Must Have	
16	The solution must provide the ability to comply to A+ Certification at the click of a button	Must Have	
17	The solution must provide the ability to control SSL settings via a GUI based interface	Must Have	
18	The solution must be able to decrypt SSL web traffic for inspection without terminating or changing the HTTPS connection	Must Have	
19	The solution must provide the following features and protection: a. HTTP protocol validation b. Correlated based attack protection c. HTTP protocol attack signatures d. Cookie signing validation e. Anti-website scraping f. Whitelisting based protection g. Web worm protection h. Web application attack signatures i. Web application layer customized protection	Must Have	

20	The proposed WAF should protects against various application attacks, including: a. Layer 7 DoS and DDoS b. Brute force c. Cross-site scripting (XSS) d. Cross Site Request Forgery e. SQL injection f. Form Field and Parameter Tampering and HPP tampering g. Sensitive information leakage h. Session highjacking i. Buffer overflows j. Cookie manipulation/poisoning k. Various encoding attacks l. Broken access control m. Forceful browsing n. Hidden fields manipulation o. Request smuggling p. XML bombs/DoS	Must Have	
21	The solution must include a pre-configured list of comprehensive and accurate web attack signatures	Must Have	
22	The solution must have a database of signatures that are designed to detect known problems and attacks on web applications	Must Have	
23	The solution must be able to prevent attacks that are using Base64 encoded parameters and headers	Must Have	
24	The solution must provide signature protection against known vulnerabilities in commercial infrastructure software such as Apache, IIS and so on. The content provided by the signature detection mechanism must be based on the research done by the solution vendor threat intelligence division and a combination of other resources such as Snort, CVE and so on. This set of signatures must be continuously and automatically updated	Must Have	
25	The solution must allow administrators to add and modify signatures	Must Have	
26	The solution must support regular expressions for the following purposes: a. Signatures definition b. Sensitive data definition c. Parameter type definition d. Host names and URL prefixes definition e. Fine tuning of parameters that are dynamically learnt from the web application profile	Must Have	
27	The solution must support automatic updates to the signature database to ensure complete protection against the latest web application threats	Must Have	
28	The solution must be able to detect known attacks at multiple levels. This includes network, Web server software and application-level attacks	Must Have	
29	The solution's in-built correlation engine must address complex attacks that are ambiguous in nature. It must also examine multiple pieces of information at the network, protocol and application levels over time to distinguish between attacks and valid user traffic	Must Have	
30	The solution must inspect and monitor all HTTP(S) data and the application level including HTTP(S) headers, form fields, and the HTTP(S) body	Must Have	

31	The solution must be able to inspect HTTP requests and responses	Must Have	
32	The solution must be able to identify Web Socket connections.	Must Have	
33	The Solution must be able to parse and monitor JSON data over web socket protocol	Must Have	
34	The solution must be able to inject HTML snippet/text in the HTTP response	Must Have	
35	The solution must automatically discover HTTP traffic content type, regardless of the content-type HTTP header. With this capability, WAF should be able to parse and protect HTTP Requests with missing or wrong content-type header	Must Have	
36	The solution must be able to validate encoded data in the HTTP traffic.	Must Have	
37	The solution should protect against Deserialization attacks, accomplished by searching for signatures in the 'Request-Content' header	Must Have	
38	The solution must be able to perform validation on all types of input, including URLs, forms, cookies, query strings, hidden fields, and parameters, HTTP methods, XML elements and SOAP actions.	Must Have	
39	The solution must be capable to automatically create whitelisting/profiling of web applications.	Must Have	
40	The solution profiling technology must be able to detect and protect against threats which are specific to the custom code of the web application. After the profiling/learning phase, the solution must be able to understand the structure of each protected URL.	Must Have	
41	The solution must automatically build/learn the web application profiles and use them to detect deviations and various anomalies (or violations) and block attacks on the custom code of the application.	Must Have	
42	The solution must be able to automatically learn the web usage and application structure and elements and expected user behaviors as soon as the system is installed.	Must Have	
43	The structure and elements include URLs, directories, cookies, form fields and parameters, and HTTP methods.	Must Have	
44	User behaviors include expected value length; acceptable characters per parameter field; whether the parameter value is read-only or editable by the user and whether the parameter is mandatory or optional.	Must Have	
45	The solution must be able to automatically switch profile to the enforcement mode after a suitable learning period which can be defined manually by the administrator.	Must Have	
46	The solution profiling learning mode must be able to recognize changes to the web application and simultaneously protect web applications at the same time.	Must Have	
47	The solution must be able to learn and create profile and in parallel should protect application by blocking malicious requests using negative security model based policies.	Must Have	

48	The solution must allow profiles to be manually changed and information can be added and removed to fine tune the profiles.	Must Have	
49	The solution must support profiling from only a set of trusted users to learn the normal acceptable behavior and usage of the web application.	Must Have	
50	The solution must allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.	Must Have	
51	The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in learning mode.	Must Have	
52	The solution must be able to perform profiling of web applications in an environment where there is a mixture of good and bad traffic. The solution must be able to automatically differentiate good and bad traffic when learning the profile. Bad traffic should not be learnt	Must Have	
53	The solution must be able to automatically learn all the host names of the web applications being protected.	Must Have	
54	The solution must be able to perform profiling of JSON. HTTP requests in the JSON format must be learnt by the WAF with the parameters and values.	Must Have	
55	The solution must be able to protect web applications that include Web services (XML) content.	Must Have	
56	The XML protection offered by the solution must be similar to the web application protection provided with automated profiling/learning capability.	Must Have	
57	The solution must support custom security rules. Administrators should be able to define rules for the positive and negative security model and to create correlation rules with multiple criteria.	Must Have	
58	The solution must be able to perform virtual patching for its protected web applications.	Must Have	
59	The solution must support all the following web application vulnerability assessment tools (Web application scanners) to virtually patch web application vulnerabilities: a. Cenzic b. HP Fortify WebInspect c. IBM AppScan d. Qualys e. WhiteHat	Must Have	
60	The solution must address and mitigate the OWASP Top Ten web application security vulnerabilities. Describe how each of the OWASP Top Ten vulnerability is addressed by the solution.	Must Have	
61	The solution must support the capability to define security policies based on the threat intelligence feeds listed previously to perform the following functions: a. Alert b. Block IP c. Block Session d. Block User	Must Have	

62	The proposed WAF should be session aware and should be able to enforce and report session	Must Have	
63	The solution must be able to track and monitor web application users. This user tracking mechanism must be automated, with no changes to the existing application or authentication scheme.	Must Have	
64	The solution must support user tracking using both form-based and certificate-based user authentication.	Must Have	
65	The solution must provide automated, real-time event alert mechanism.	Must Have	
66	The solution must be able to monitor and block users when required.	Must Have	
67	The solution must support masking of sensitive data in alerts.	Must Have	
68	The solution must support sending of logs in CEF standard.	Must Have	
69	The solution must support a flexible set of follow-up actions to be taken in the event of an alert generation. For example, if an alert is generated based on a Policy, send an email to Administrator X and Manager Y followed by sending a syslog to Destination 1 and a CEF-formatted log to Destination 2.	Must Have	
70	Should support manual as well as automatic online updation of the Signatures	Must Have	
71	Signature updation should be independent of the underlying firmware OS	Must Have	
72	Signature updation should be not cause any downtime	Must Have	
73	The proposed WAF should protect from HPP attacks	Must Have	
74	The proposed WAF should support Policy Evasion Detection Engine	Must Have	
75	The proposed WAF should be able to do Manipulation of invalidated input	Must Have	
76	The proposed WAF should protect against Remote File Inclusion Attacks	Must Have	
77	The proposed WAF should protect against requests for restricted object and file types	Must Have	
78	The proposed WAF should protect unauthorized navigation	Must Have	
79	The proposed WAF should protect against Directory/Path traversal	Must Have	
80	The proposed WAF should protect against known worms and vulnerabilities	Must Have	
81	The proposed WAF should prevent OS and web server fingerprinting	Must Have	
82	The proposed WAF should conceal any HTTP error messages from users	Must Have	
83	The proposed WAF should remove application error messages from pages sent to users	Must Have	
84	The proposed WAF should prevent leakage of server code	Must Have	
85	The proposed WAF should support Schema validation	Must Have	
86	The proposed WAF should support Parser protection (XML Bombs, Recursion Attacks)	Must Have	
87	The proposed WAF should support XPATH injection	Must Have	

88	The proposed WAF should support RSS/Atom feed injection	Must Have	
89	The proposed WAF should support XML islands	Must Have	
91	The proposed WAF should be capable to trigger a script based on an event	Must Have	
92	The proposed WAF should support staging of policies/attack signatures before being enforced. The staging to automatic enforcing time period should be customizable	Must Have	
93	The proposed WAF should provide application-specific XML filtering and validation functions that ensure the XML input of web-based applications is properly structured. It should provide schema validation, common attacks mitigation, and XML parser denial-of-service prevention.	Must Have	
94	The WAF must be able to inject a JavaScript challenge instead of the original response in order to test whether the client is a legitimate browser or a bot	Must Have	
Reporting Features			
1	The system must be able to display attacks and its mitigation statistics	Must Have	
2	The system must equip with a high-speed logging mechanism which can send log message in near real-time without significantly impacting system performance.	Must Have	
4	The system shall have ability to identify and notify system faults and loss of performance (SNMP, syslog, e-mail, etc)	Must Have	
5	The system shall have ability to customize logging	Must Have	
6	The system must provide request logging that support profile by enabling configuration log entries to be reported when requests/responses are received, supports audit logging of HTTP/decrypted HTTPS requests/responses, and enables specification of a response to be issued when a specific requests/responses occur.	Good to Have	
7	The system must provide response logging so that it helps in analyzing responses is especially useful when logging response-related security events, such as Data Guard or response signatures, it is also be useful in analyzing request violations, to determine whether they represent an actual attack or a false positive	Good to Have	
8	The system shall have ability to generate service and system statistics. Provides dashboard displays anomaly statistics about number attacks, dropped requests, a summary of system traffic.	Good to Have	
9	The system must provide high-level view of recent activity in a single screen, where you can view aggregated events (incidents) rather than individual transactions (that are displayed on the Requests screen). Incidents are suspected attacks on the web application.	Must Have	
10	The system shall be capable of logging security events with Syslog	Must Have	
11	The system shall be capable of logging security events with SNMP as well as SNMP MIB is polled for information about any current active attacks	Must Have	

12	The system must provide built in logging to 3rd party security event tracking systems such as SIEM like Arcsight or Splunk	Must Have	
13	The proposed solution should have the capability to capture tcpdump for forensic analysis.	Must Have	
14	The proposed solution should have the capability to create a granular logging policy per application.	Must Have	
15	The proposed solution should have the capability to define a customized log format for each application.	Must Have	
16	The proposed solution should have the capability to define multiple log destinations for each application	Must Have	
17	The solution must provide pre-packaged reporting capabilities out-of-the-box without user intervention/further configuration: a. Alert analysis (For Application user, Known attack patterns, severity, Source IP with severity & type, URL, User with severity & type, Violation Types) b. Daily & weekly Top 10 WAF violations c. Daily Summary Blocked Connections d. Data Leakage Report e. Directory Browsing Detection Report f. List of Alerts g. PCI - WAF violations h. Sensitive Error Messages Leakage Report i. Slow HTTP/S Alerts	Must Have	
18	The solution must have the functionality within the UI out-of-the-box that enables the administrator to create custom report templates based on the existing out-of-the-box reports.	Must Have	
19	The solution must support automatic generation of reports based on a defined schedule.	Must Have	
20	The solution must support scheduling of report generation to start only at a future date.		
Management			
1	Proposed hardware solution should have a dedicated out-of-band management port	Must Have	
2	Proposed solution should have Web GUI (HTTPS) for management. The solution must allow the user to use a standard browser to access the management UI	Must Have	
3	Proposed solution should have CLI (SSH) for management	Must Have	
4	Proposed solution should have the capability to restrict SSH from specific IP address	Must Have	
5	Proposed solution should have the capability to restrict Shell access tp specific users	Must Have	
6	Proposed solution should have the capability to define an ACL for Web/CLI access	Must Have	
7	Proposed solution should have the detailed Access logs for audit trail purpose	Must Have	
8	The system must support Network Time Protocol (NTP) to synchronize its clock with an NTP server	Must Have	
9	The entire solution must be centrally managed for day to day operations. The management server must centrally manage all the appliances.	Must Have	

10	Reporting, policy creation, alerts management, web application protection configuration, etc must be managed from the management server.	Must Have	
11	The proposed solution should have Role based access	Must Have	
12	The solution must provide Role-Based Access Control. It should at minimum have the below user roles that facilitate separation of duties. a. Administrator b. Manager c. Auditor d. Operator e. SSL Certificate Manager f. Guest	Must Have	
13	The solution must support the following authentication mechanism for accessing the solution management UI: - In-built authentication in the solution - LDAP - RADIUS	Must Have	
14	The solution must support the following password management capabilities without relying on any external system: a. Password validity period in days b. Password length (minimum required number of characters in the password.) c. Whether a password must be significantly different from the last password used d. Whether a password must include capital letters, numbers, lower case letters and non-alphanumeric characters or not.	Must Have	
15	The solution must be able to support the configuration of the following lockout settings from the solution management UI: a. Login failed attempts period (in minutes) in which entering an incorrect password multiple times locks an account b. Number of failed login attempts which result an account to be locked c. Lock duration in minutes	Must Have	
16	The solution must support the capability of trust-based communication between the different components in the solution. i.e. Communication between solution components needs to be done using certificates.	Must Have	

The bidder is required to provide exhaustive list of the hardware, software, etc to implement the project.

Dated this…… Day of……..2019

(Signature)

(Name) (In the capacity of)
Duly authorized to sign Bid for and on behalf of

Annexure L - Client Reference

NPCI/RFP/2018-19/IT/17 dated 25.02.2019

Sr.No	Particulars	Details
1	Name of the Organization	
2	Contact Person Name and Designation	
3	Phone Number of the Contact person	
4	Email Address of the Contact person	

(Signature)

(Name) (In the capacity of)
Duly authorized to sign Bid for and on behalf of

Section 12 - Documents to be put in Envelope 'C'

Annexure M –Commercial Bid Form

(To be included in Commercial Bid Envelope)

To

NPCI

Dear Sirs,

Re: RFP No. NPCI/RFP/2018-19/IT/17 dated 25.02.2019 for "Request for Proposal for supply and installation of Web Application Firewall".

Having examined the Bidding Documents placed along with RFP, we, the undersigned, offer to provide the required infrastructure in conformity with the said Bidding documents for the sum of Rs.……..(Rupees_____) (exclusive of taxes) or such other sums as may be ascertained in accordance with the Schedule of Prices attached herewith and made part of this Bid.

We undertake, if our Bid is accepted, to provide _____ for the above purpose within the stipulated time schedule. We agree to abide by the Bid and the rates quoted therein for the orders awarded by NPCI up to the period prescribed in the Bid which shall remain binding upon us. 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 against fraud and corruption in force in India.

We have complied with all the terms and conditions of the RFP. We understand that you are not bound to accept the lowest or any Bid you may receive.

Dated this…… Day of……..2019

(Signature)

(Name) (In the capacity of)

Duly authorized to sign Bid for and on behalf of

Annexure N - Commercial Bid

RFP # NPCI/RFP/2018-19/IT/17 dated 25.02.2019

(On Company Letter head)

Sr	Equipment	Units Required	Unit cost with 1 year onsite OEM warranty	Total Units Cost	AMC Unit cost for 2nd Year	Total AMC for 2nd Year	AMC for 3rd Year	AMC Unit cost for 3rd Year	Grand total
			(INR)	(INR)	(INR)	(INR)	(INR)	(INR)	(INR)
	A	B	C	D = C*B	E	F=E*B	G	H=G*B	I = D+F+H
1	Hardware and support	4							
2	One time Implementation								
3									
4									
5									
6									

- AMC cost should not be less than **8%** of the cost of hardware / software
- The bidder shall meet the requirements of applicable Goods & Services Tax (GST)
- Delivery locations would be as per clause 8.8 of the RFP

TCO =

(Amount in Rs)

All prices are exclusive of taxes.

Dated this…… Day of……..2019

(Signature)

(Name) (In the capacity of)
Duly authorized to sign Bid for and on behalf of

Annexure O - Bill of Material

NPCI/RFP/2018-19/IT/17 dated 25.02.2019

Line Item Wise Prices (Details of all line items of the Commercial Bid, including AMC charges)

Line Item	Item Name / Part No	Description	Unit Price including 1 year warranty	2nd Year-AMC	3rd Year-AMC	Sub Total	Quantity	Total Price
1								
2								
3								
4								
5								
6								

- Delivery locations would be as per clause 8.8 of the RFP

Annexure Z - Non-Disclosure Agreement

This Agreement is made and entered on this -------- day of ----------, 2019 (**"Effective Date"**) between

NATIONAL PAYMENTS CORPORATION OF INDIA, a company incorporated in India under Section 25 of the Companies Act, 1956 (Section 8 of the Companies Act, 2013) and having its registered office at **1001A, B Wing, 10th Floor, The Capital, Plot 70, Block G, Bandra-Kurla Complex, Bandra (East), Mumbai - 400 051, Maharashtra**, CIN: U74990MH2008NPL189067 (Hereinafter referred to as **"NPCI"**, which expression shall mean and include unless repugnant to the context, its successors and permitted assigns);

AND

_____, a company registered in _____and having its registered office at _____ (Hereinafter referred to as "-------", which expression shall mean and include unless repugnant to the context, its successors and permitted assigns).

The term "Disclosing Party" refers to the party disclosing the confidential information to the other party of this Agreement and the term "Receiving Party" means the party to this Agreement which is receiving the confidential information from the Disclosing Party.

NPCI and --------- shall hereinafter be jointly referred to as the "Parties" and individually as a "Party".

NOW THEREFORE

In consideration of the mutual protection of information herein by the parties hereto and such additional promises and understandings as are hereinafter set forth, the parties agree as follows:

Article 1: Purpose
The purpose of this Agreement is to maintain in confidence the various Confidential Information, which is provided between NPCI and ------ to perform the considerations (hereinafter called "Purpose") set forth in below:

RFP for supply and installation of Web Application Firewall

Article 2: DEFINITION
For purposes of this Agreement, "**Confidential Information**" means the terms and conditions, and with respect to either party, any and all information in written, representational, electronic, verbal or other form relating directly or indirectly to the Purpose (including, but not limited to, information identified as being proprietary and/or confidential or pertaining to, pricing, marketing plans or strategy, volumes, services rendered, customers and suppliers lists, financial or technical or service matters or data, employee/agent/ consultant/officer/director related personal or sensitive data and any information which might reasonably be presumed to be proprietary or confidential in nature) excluding any such information which (i) is known to the public (through no act or omission of the Receiving Party in violation of this Agreement); (ii) is lawfully acquired by the Receiving Party from an independent source having no obligation to maintain the confidentiality of such information; (iii) was known to the Receiving Party prior to its disclosure under this Agreement; (iv) was or is independently developed by the Receiving Party without breach of this Agreement; or (v) is required to be disclosed by governmental or judicial order, in which case Receiving Party shall give the Disclosing Party prompt written notice, where possible,

and use reasonable efforts to ensure that such disclosure is accorded confidential treatment and also to enable the Disclosing Party to seek a protective order or other appropriate remedy at Disclosing Party's sole costs. Confidential Information disclosed orally shall only be considered Confidential Information if: (i) identified as confidential, proprietary or the like at the time of disclosure, and (ii) confirmed in writing within Seven (7) days of disclosure.

Article 3: NO LICENSES

This Agreement does not obligate either party to disclose any particular proprietary information; to purchase, sell, license, transfer, or otherwise dispose of any technology, services, or products; or to enter into any other form of business, contract or arrangement. Furthermore, nothing contained hereunder shall be construed as creating, conveying, transferring, granting or conferring by one party on the other party any rights, license or authority in or to the Confidential Information disclosed under this Agreement.

Article 4: DISCLOSURE

1. Receiving Party agrees and undertakes that it shall not, without first obtaining the written consent of the Disclosing Party, disclose or make available to any person, reproduce or transmit in any manner, or use (directly or indirectly) for its own benefit or the benefit of others, any Confidential Information save and except both parties may disclose any Confidential Information to their Affiliates, directors, officers, employees or advisors of their own or of Affiliates on a "need to know" basis to enable them to evaluate such Confidential Information in connection with the negotiation of the possible business relationship; provided that such persons have been informed of, and agree to be bound by obligations which are at least as strict as the recipient's obligations hereunder. For the purpose of this Agreement, Affiliates shall mean, with respect to any party, any other person directly or indirectly Controlling, Controlled by, or under direct or indirect common Control with, such party. "Control", "Controlled" or "Controlling" shall mean, with respect to any person, any circumstance in which such person is controlled by another person by virtue of the latter person controlling the composition of the Board of Directors or owning the largest or controlling percentage of the voting securities of such person or by way of contractual relationship or otherwise.

2. The Receiving Party shall use the same degree of care and protection to protect the Confidential Information received by it from the Disclosing Party as it uses to protect its own Confidential Information of a like nature, and in no event such degree of care and protection shall be of less than a reasonable degree of care.

3. The Disclosing Party shall not be in any way responsible for any decisions or commitments made by Receiving Party in relying on the Disclosing Party's Confidential Information.

Article 5: RETURN OR DESTRUCTION OF CONFIDENTIAL INFORMATION

The parties agree that upon termination of this Agreement or at any time during its currency, at the request of the Disclosing Party, the Receiving Party shall promptly deliver to the Disclosing Party the Confidential Information and copies thereof in its possession or under its direct or indirect control, and shall destroy all memoranda, notes and other writings prepared by the Receiving Party or its Affiliates or directors, officers, employees or advisors based on the Confidential Information and promptly certify such destruction.

Article 6: INDEPENDENT DEVELOPMENT AND RESIDUALS

Both parties acknowledge that the Confidential Information coming to the knowledge of the other may relate to and/or have implications regarding the future strategies, plans, business activities, methods, processes and or information of the parties, which afford them certain competitive and strategic advantage. Accordingly, nothing in this Agreement will prohibit the Receiving Party from developing or having developed for it products, concepts, systems or techniques that are similar to or compete with the products, concepts, systems or techniques contemplated by or embodied in

the Confidential Information provided that the Receiving Party does not violate any of its obligations under this Agreement in connection with such development.

Article 7: INJUNCTIVE RELIEF

The parties hereto acknowledge and agree that in the event of a breach or threatened breach by the other of the provisions of this Agreement, the party not in breach will have no adequate remedy in money or damages and accordingly the party not in breach shall be entitled to injunctive relief against such breach or threatened breach by the party in breach.

Article 8: NON-WAIVER

No failure or delay by either party in exercising or enforcing any right, remedy or power hereunder shall operate as a waiver thereof, nor shall any single or partial exercise or enforcement of any right, remedy or power preclude any further exercise or enforcement thereof or the exercise of enforcement of any other right, remedy or power.

Article 9: DISPUTE RESOLUTION

If any dispute arises between the parties hereto during the subsistence or thereafter, in connection with or arising out of this Agreement, the dispute shall be referred to arbitration under the Indian Arbitration and Conciliation Act, 1996 by a sole arbitrator mutually agreed upon. In the absence of consensus about the single arbitrator, the dispute may be referred to joint arbitrators, one to be nominated by each party and the said arbitrators shall nominate a presiding arbitrator, before commencing the arbitration proceedings. Arbitration shall be held in Mumbai, India. The proceedings of arbitration shall be in the English language. The arbitrator's award shall be final and binding on the parties.

Article 10: GOVERNING LAW AND JURISDICTION

This Agreement shall be governed exclusively by the laws of India and jurisdiction shall be vested exclusively in the courts at Mumbai in India.

Article 11: NON-ASSIGNMENT

This Agreement shall not be amended, modified, assigned or transferred by either party without the prior written consent of the other party.

Article 12: TERM

This Agreement shall remain valid from the effective date until the termination of this Agreement. The obligations of each Party hereunder will continue and be binding irrespective of whether the termination of this Agreement for a period of three (3) years after the termination of this Agreement.

Article 13: INTELLECTUAL PROPERTY RIGHTS

Neither Party will use or permit the use of the other Party's names, logos, trademarks or other identifying data, or infringe Patent, Copyrights or otherwise discuss or make reference to such other Party in any notices to third Parties, any promotional or marketing material or in any press release or other public announcement or advertisement, however characterized, without such other Party's prior written consent.

Article 14: GENERAL

1. Nothing in this Agreement is intended to confer any rights/remedies under or by reason of this Agreement on any third party.

2. This Agreement and the confidentiality obligations of the Parties under this Agreement supersedes all prior discussions and writings with respect to the Confidential Information and constitutes the entire Agreement between the parties with respect to the subject matter hereof. If any term or provision of this Agreement is determined to be illegal, unenforceable, or invalid in whole or in

part for any reason, such illegal, unenforceable, or invalid provisions or part(s) thereof shall be stricken from this Agreement.

3. Any breach of any provision of this Agreement by a party hereto shall not affect the other party's non-disclosure and non-use obligations under this Agreement.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement by their duly authorized representatives as of the Effective Date written above.

NATIONAL PAYMENTS CORPORATION OF INDIA	**TYPE COMPANY NAME**
By: Name:	By: Name:
Designation:	Designation: