

Broad Scope of Work:

The Bank hereafter termed as “**Insured** “ by the virtue of this RFP intends to procure quotations inclusive of suitable insurance covers for indemnifying losses incurred by the bank directly or indirectly on account of cyber crime or any other activities conducted by any party by the aid of technological platform with a malicious intent .

The cover provided by the bidders should be inclusive of all e-transactions of the insured and should be extended to cover transactions on the medium of applications and third party interface / integrations involving the insured i.e.: All communication / money transfer/ transaction based channels should be covered like ATM, Internet Banking, UPI (Unified Payment Interface), Mobile banking, Mobile Wallet, BHIM app and other payment applications like POS etc.





The limit of Indemnity: The covers to be provided by the bidders should be designed to indemnify losses incurred of the insured as per the below mentioned limits:

- | | | |
|----|--------------------------|---------------|
| a. | Any one accident : (AOA) | Rs 50 crores |
| | Any one year: (AOY) | Rs 50 crores |
| b. | Any one accident : (AOA) | Rs 75 crores |
| | Any one year: (AOY) | Rs 75 crores |
| c. | Any one accident : (AOA) | Rs 100 crores |
| | Any one year: (AOY) | Rs 100 crores |

The bids submitted by the participating insurers should be inclusive of premium quotes for atleast one of categories (ie a or b or c) . In case the insurer intends to submit quotes for all three categories they can submit the same by distinctly separating the premiums.

The covers provided by the bidders should indemnify the losses incurred by the insured during the policy period against all the below mentioned conditions:

DATA LIABILITY

-  Loss of Personal Information
-  Loss of corporate information
-  Outsourcing
-  Network security

ADMINISTRATIVE OBLIGATIONS

- ✚ Data Administrative Investigation – Insurer will pay on behalf insured all professional fees for legal advice and representation in connection with any regulatory investigation.
- ✚ Data Administrative Fines – Insurer will pay on behalf of any insured all Data administrative fines that the insured is legally obligated to pay on the conclusion of a regulatory investigation arising out of breach of Data Protection Law

REPUTATION AND RESPONSE COSTS- The insurer will pay on behalf of the insured the costs incurred while undertaking any of the below mentioned activities at the instance of a claim

- ✚ Pro-active Forensic Services
- ✚ Repair of Company's reputation
- ✚ Repair of individual reputation
- ✚ Notification to Data Subjects
- ✚ Monitoring
- ✚ Electronic data

MULTIMEDIA LIABILITY /SOCIAL MEDIA LIABILITY

CYBER/PRIVACY EXTORTION- The insurer will pay on behalf of the insured all extortion loss to the limit of indemnity which the insured incurs solely as a result of extortion threat

NETWORK INTERRUPTION- The insurer will pay the insured any network loss up to the limit of indemnity in respect of material interruption that an insured incurs after the waiting period has expired and solely as a result of security failure.

Any attempt resulting in the disruption of network partially or totally and costs incurred to repair the network to be included in the limit of liability

The covers submitted by the bidders should be inclusive various kinds of losses mentioned below but not confined to:

- ✚ E THEFT LOSS- The insurer will pay all the losses incurred by the Bank and related parties (Bank customers / vendors / associates) up to the limit of indemnity on account of E Theft.
 - ✚ E COMMUNICATION LOSS
 - ✚ THREAT LOSS
 - ✚ E VANDALISM LOSS
 - ✚ E BUSINESS INTERRUPTION LOSS
-

The insurer may please specify if there is cover provided against each of the following. In case any of the below items are not covered please indicate accordingly.

- ✓ Hacking
 - ✓ Phishing
 - ✓ Keystroke login or Key Logging
 - ✓ Viruses
 - ✓ Worms
 - ✓ Trojans
 - ✓ Bots
 - ✓ Spyware
 - ✓ DNS Cache poisoning
 - ✓ Malware based attacks
 - ✓ Ransom ware
 - ✓ Denial of Service (DOS) attacks
 - ✓ Watering hole
 - ✓ Cyber Terrorist Acts
-

Online card frauds:

Liability incurred by the bank on account of loss of sensitive data pertaining to cards issued to bank account holders leading to monetary claims excluding negligence and misconduct by the account holder.

The covers submitted by the bidding companies should indemnify losses incurred by the insured on account of any technological advancement / software / code / application / created by any party with a malicious intent over and above the abovementioned mode of attacks

The scope of cover provided by bidders should cover the below mentioned aspects in the instance of a claim:

Property and Theft:

- Partial or complete damage to the networking and transactional based model of the banking software
- Loss of data of the bank / records / confidential information/sensitive information of bank account holders , internal banking transactions, bank policies , interbank transactions
- Partial or complete damage to electronic media and data contents
- **All SWIFT transactions to be covered**

- Crisis Management and response to data theft (includes costs of administrative expenses i.e. forensic investigations, penalties, regulatory and governmental fines)

The covers submitted by the bidders to be inclusive of situation based / transaction based losses:

- System Issue due to which customers could view account details of other customers through Internet banking
- Defamatory content posted in the bank's Mobile App by exploring weakness in the application.
- Email id of Bank's customer hacked – Fund Transfer request received and processed by the bank – disowned by the customer
- Data Leakage by a resigned, retired or Serving Employees
- Extortion money demands by cyber criminals in possession of critical data, or having a handle on important internal IT apps, capable of bringing down the IT infrastructure.
- Alteration, Damage, Deletion or destruction of data owned by the bank or for which bank is legally liable. Cost arising out of blank media, increased labour
- Outside malicious attack (NOT technical failure) on important WAN devices of bank such as Firewall, Routers, causing application non-availability, causing loss of profit
- Service provider network downtime, causing application non-availability, causing loss of profit
- Bank employee acting on legitimate looking transaction instructions from customer, and transferring money to fraudster's account. Phishing / 'Fake President' frauds
- Customer transferring money based on legitimate looking communication from the Bank. Subsequent loss to the customer & bank
- Malicious code/virus inserted by hacker, in bank's systems/software, triggering automatic money transfer from branch account (or any other account) to hacker's account
- Money transferred from an account by the customer to a recipient, but NOT debited in sender's account - Using malicious code to make the software misbehave
- Virus in the bank network making the ATM machines spew of cash
- Intentional fraud carried out by an existing or ex-employee, using cyber/IT systems as the attack vector.