CORPORATE OFFICE: BANGALORE
CREDIT MONITORING & REVIEW DEPARTMENT
Ph No. 080-22356195 :: FAX 080-22268718

Ref: 002/2921/2019/CMRD/Clarifications-RFP-0145 **Date: JAN 08, 2019**

To,
All participating Bidders.

SUB: Bank's reply to the further queries raised by some of the bidders.
Ref: 1) RFP 0145/CO: CMRD/EWS_Procurement Date: 10.12.2018
2)151/2921/2018/CMRD/Clarifications-RFP-0145 Date: Dec. 29, 2018
3)001/2921/2019/CMRD/Clarifications-RFP-0145 Date: JAN 04, 2019

List of Items deleted from the Scoring Evaluation Approach		
Sl No.	Functional/Technical Requirements	Remarks
1.47	Proposed Solution should be able to consume externally sourced entity information (e.g. IP addresses, destination accounts etc.) to identify known fraudulent activity. The system should also have the facility to export the entity data corresponding to confirmed fraud cases within the bank so that the data can be shared with external agencies like regulators, banker's association. The system should be able to download/extract data from other agencies line regulators, Credit rating agencies, ROC, SROs, SEBI, CERSAI, NCLT, District/High/Supreme Court, Credit information Agencies, ECGC, other banks, Media, Income Tax, Sales Tax, GST, Central Excise etc	IP addresses, destination accounts etc. are not related to EWS - Removed
8.16	The system should have the feature such that the bank should be able to do following actions based on response (fraud detection): 1. Deny/allow transaction. 2. Generate alerts to the monitoring team. 3. Provide reports stating all facts and figures of operations	Deny/allow transaction is not part of EWS - Removed
1.11	The solution should support cross-channel rules and alert i.e. consider activity online and on offline	Part of FRMS - Removed
1.31	The rules engine should use updatable user defined tables as decision elements such as: Negative and / or positive files (lists / IP Addresses)	Part of FRMS - Removed
1.46	Proposed solution should have the ability to monitor all pre-login, login and post login transactions to detect any suspicious patterns	Part of FRMS - Removed
2.2	The solution should support model score transactions across multiple channels by staff, customer and channel attributes and across products	Part of FRMS - Removed

2.3	The solution should have capability to include rule/model alerts combined into an Entity level Alert. For example, Entities may include: transactions, customers, accounts etc	Part of FRMS - Removed
2.8	The solution should support tracking leveis include Transaction, Card, Account, Customer, Customer Groups, etc. The solution should also enable the user to uptoad signals in some of the points, which require attention	Part of FRMS - Removed
2.9	The solution should support grouping capabilities as dimensions for trending, e.g. regional, merchant type, customer type, temporal, etc.	Part of FRMS - Removed
2.14	The solution should have ability to define clusters using several different techniques and relations	Part of FRMS - Removed
2.18	The solution should provide complete evidence as to why a transaction was declined/hold	Part of FRMS - Removed
2.19	The Solution should be able to provide both real—time transaction monitoring and transaction blocking/hold feature for suspicious core banking transactions	Part of FRMS - Removed
2.21	Solution should cover other behavioural aspects than per user, e.g. per account behaviour , per beneficiary/receiver behaviour, per IP—address behaviour, per device behaviour	Part of FRMS - Removed
3.12	The solution should support detailed Threshold Analysis, in order to fine tune alerts and reduce false positives	Part of FRMS - Removed
8.1	The solution should be able to get all the transactional logs like money transfer, bill pay as well as any profile change transactions etc on a real time or offline manner, market data, other agency data. regulator data, other government department data for the risk engine to analyse and calculate the risk value of the transaction and build case for Fraud Analysis and further manual risk analysis	Part of FRMS - Removed
8.2	The Solution should have a comprehensive out-of-the—box rules for each channel/across channels	Part of FRMS - Removed
8.3	The solution should have the capability for Device-ID check and User-Device ID association check and solution should provide functionality to register the device(s) for the first time	Part of FRMS - Removed
8.4	The solution should detect too many transactions from the same user (User Velocity) or from the same device (Device velocity, Beneficiary Velocity) within a time—Interval and different location	Part of FRMS - Removed
8.5	The solution should have capability for Zone-hopping Check, have capability for Trusted IP check, have the capability for Trusted Aggregator check	Part of FRMS - Removed
8.8	Risk Engine should be configurable for learning only mode or production mode. Bank should be able to switch on this based on their convenience	Part of FRMS - Removed
8.9	The solution should support analysis of common point of compromise (CPC) and also possible points of compromise. it should support automated way of identifying point of compromise like system, user ,ISP etc and it should also have the capability to de-dupe and provide suspect compromised accounts basis the identified point of compromise	Part of FRMS - Removed
8.11	The APIs, Back Office applications, and databases should support creating rules using internet Protocol Version 6 (va6) addresses in addition to IPv4 addresses.	Part of FRMS - Removed

8.12	The solution should have inbuilt auditing and logging functionality. All events should be logged and be available to support investigation related to fraud incidents and other uses.	Part of FRMS - Removed
8.17	Multi tenancy support and Data segregation should be available.ie multiple section of the bank should be able to monitor their systems independently. The application should support global and tenant specific rules	Part of FRMS - Removed
8.19	Should be able to restrict/allow transactions based on IP address, City, country, ZIP Code, and any other geographic variables, terminal Ed (URL I mobile number etc). It should also be possible to define any dynamic variable which could be part of overall message set for restricting/monitoring transactions	Part of FRMS - Removed
8.20	Support detection of both wired and wireless fraud related based on IP and anomaly in transaction content due to MitM or MitB attacks. The solution should support the ability to track behaviour based on IP address. Support cross border/multi currency transactions	Part of FRMS - Removed
8.21	Should check for URL tampering while the request is sent for authentication/authorization.	Part of FRMS - Removed
8.22	Should support Velocity checks (user and device).	Part of FRMS - Removed
8.24	The solution should be capable of identifying the country of origin and destination based on defined parameters and filters the transaction through country specific regulations	Part of FRMS - Removed
8.25	The solution should have provisions for hosting country specific risk assessment and fraud monitoring rules and apply the same at the time of transaction passing through the solution	Part of FRMS - Removed
8.27	The system should have the capability to self-control false positives and false negatives. The alerts should give the origin/source of information	Part of FRMS - Removed
8.28	The solution should assist in detecting suspicious activity and anomalous changes in transaction activity patterns, and help reduce false-positive alerts	Part of FRMS - Removed
8.30	All the criteria of the monitoring module are configured by combining the programmed rules of operations and variable parameters. The programmed rules of operations may include the identification, by the system, of such transgressions as the following: 1. Transactions across multiple countries/ geographies within specified time frame. 2. Multiple transactions / concentration of usage at the same merchant or group of merchants especially high risk MCCs. 3. Repeated unsuccessful attempts at entering PIN. 4. Every transaction must be given a score, based on the rules defined in Fraud & Risk Monitoring and Management System. 5. Should support detection of pre-authorizations & authorizations and assign risk scores accordingly for approval or decline of the transaction 6. Should manage risk at the portfolio Eevel in real-time / near real—time	Part of FRMS - Removed
8.31	Should be able to interface with authorization systems and processes to address improper transactions before, during or immediately after they occur. OEM should provide interface Apls	Part of FRMS - Removed

8.35	The Simulators should be capable of testing what if scenarios assess conflicts in multiple rule configurations and also help test efficiency of the rules.	Part of FRMS - Removed
8.37	The system should have a tool that can be used to view, add, modify, delete, or confirm transaction information online based on the scenario	Part of FRMS - Removed
8.44	Few of the rules that the risk engine should monitor & deploy to throw alerts are mentioned as under:	Part of FRMS - Removed
8.45	IP checks: De-duplication Fraudulent IPs and decline transactions	Part of FRMS - Removed
8.46	Velocity Checks	Part of FRMS - Removed
8.47	Device authentication checks	Part of FRMS - Removed
8.48	Risk Scoring based on rules deployed to accept or reject transactions	Part of FRMS - Removed
8.49	Award high score to those transactions originated from countries where KYC compliance is low	Part of FRMS - Removed
8.50	Country/ Geographic de-duplication	Part of FRMS - Removed
8.58	Support maintenance of negative/positive lists of merchants/customers/cards etc	Merchants and Cards are not relevant for EWS - Removed
8.62	The Solution should have comprehensive alerts management with severity as per set parameters and send the same to addressees by SMS, E—mail, IVRs or off-line through messages/reports etc	IVRs not relevant for EWS - Removed

Note: All other Terms and conditions of RFP will remain the same. Also, Last Date & Time for submission of Bids in **Online Mode** will remain the same as **18/01/2019 up to 16:00 hours** & Last Date & Time for submission of Physical Documents (**Offline Mode**) will remain the same as **21/01/2019 up to 16:00 hours.**

Yours faithfully,

General Manager

- 0 O 0 -