Pre bid replies for RFP. Ref. No. : RFP-01/2020-DBS-257/IBPGS-25/CI/2020 dated 20th February 2020 - for RFP - Renewal of Crime insurance Policy under Non-Traditional Insurance Policies from 1st April 2020 to 31st March 2021

Sl No.	QUERY	REMARKS
	INSURANCE PROGRAM	
1.	Claim Details Experienced in the last 2 years (2018-19 and 2019-20) – CANARA BANK No. of claims reported: Nature of Claim: Date of Discovery: Location: Amount of Loss: Claim Amount Paid:	2018-19 and 2019-20 Nature of claims: The claims pertain to unauthorized fraudulent transactions pertaining to Internet Banking, Mobile Banking, UPI and ATM liability shift transactions. Date of Discovery: various dates during the policy period. Location: various locations pan India.

2018 - 19 Policy (Policy No. 120400/36/18/17/00000002)

	Description	Shift Liability Claim		UPI Fraud Claims		Internet & Mobile Banking		Total	
		Count	Amount	Count	Amount	Count	Amount	Count	Amount
1	Rejected	1	0	0	0	0	0	1	0
2	Settled	0	0	0	0	0	0	0	0
3	Under Process	0	0	0	0	2	5905096	2	5905096
4	Outstanding	0	0	2	2328215	1	900000	3	3228215
	Total Reported	**1**	**0**	**2**	**2328215**	**3**	**6805096**	**6**	**9133311**
	INCURRED CLAIMS	**0**	**0**	**2**	**2328215**	**3**	**6805096**	**6**	**9133311**

2019- 20 Policy (Policy No. 120400/36/19/17/00000001)									
	Description	Shift Liability Claim		UPI Fraud Claims		Internet & Mobile Banking		Total	
		Count	Amount	Count	Amount	Count	Amount	Count	Amount
1	Rejected	0	0	0	0	0	0	0	0
2	Settled	0	0	0	0	0	0	0	0
3	Under Process	0	0	0	0	2	288480	2	288480
4	Outstanding	1	4652300	4	568088	6	5788676	11	11009064
	Total Reported	**1**	**4652300**	**4**	**568088**	**8**	**6077156**	**13**	**11297544**
	INCURRED CLAIMS	1	4652300	4	568088	8	6077156	13	11297544

2.	Claim Details Experienced in the last 2 years (2018-19 and 2019-20) – SYNDICATE BANK No. of claims reported: Nature of Claim: Date of Discovery: Location: Amount of Loss: Claim Amount Paid: Post Loss Measures Taken:	2018-19 and 2019-20 Nature of claims: The claims pertain to unauthorized fraudulent transactions pertaining to Internet Banking, Mobile Banking, UPI and ATM liability shift transactions. Date of Discovery: various dates during the policy period. Location: various locations pan India.

केनरा बैंक ★ CANARA BANK ★ Internet & Payment Gateway Section ★ H.O., Bengaluru

2018 - 19 Policy

	Description	Mobile Banking / UPI		Internet Banking		Total	
		Count	Amount	Count	Amount	Count	Amount
1	Under Process	2	5,00,000	1	2,20,000	3	7,20,000
2	Settled	0	0	0	0	0	0
3	Rejected	0	0	0	0	0	0
4	Outstanding	0	0	0	0	0	0
	Total Reported	**2**	**5,00,000**	**1**	**2,20,000**	**3**	**7,20,000**

2019- 20 Policy

	Description	Mobile Banking / UPI		Internet Banking		Total	
		Count	Amount	Count	Amount	Count	Amount
1	Under Process	0	0	1	14,07,000	1	14,07,000
2	Settled	0	0	0	0	0	0
3	Rejected	0	0	0	0	0	0
4	Outstanding	0	0	0	0	0	0
	Total Reported	**0**	**0**	**1**	**14,07,000**	**1**	**14,07,000**

3.	Brief Description on EMV Liability Shift Claims	The liability arising due to fraudulent transaction done using other Bank card used at non EMV Canara Bank ATM's where skimming has occurred.
4.	Whether expiring policy coverages are same as mentioned in RFQ	Yes

केनरा बैंक ★ CANARA BANK ★ Internet & Payment Gateway Section ★ DBS Wing, H.O., Bengaluru - 560 001 ★ इंटरनेट भुगतान गेटवे अनुभाग, डि.बैं.से. विभाग, प्र.का., बेंगलूरु

BUSINESS OPERATIONS & MERGER		
1.	Procedure used to issue and authorize fund transfer instructions	Internet Banking retail users are provided with financial role upon registration of Internet Banking. In order to initiate fund transfers, the retail customer is required to login to Internet Banking application with the user id and login password. To authorize the fund transfer, customer has to enter the transaction password and OTP. The retail customer has to hold an active debit card to generate the transaction password. Corporate customers have to approach the branch for registration and they are provided with login user id / password and transaction password to initiate and authorize fund transfers.
2.	International Operations – Total no. of branches	5
3.	Does the bank outsource any of its operations? Provide details	The centralized reconciliation of all digital banking channels is outsourced under the direct supervision of the respective channel owners.
4.	Elaborate the scope of bulk file transactions	Bulk file transactions facilitate the corporate customers to perform Bulk Transactions without adding any Beneficiary. User can make use of this facility for Internal fund transfer within Canara Bank, NEFT and RTGS User can upload up to 25 files per day. Each file can contain up to 1000 Transactions with up to a limit of 1 Crore. Maker/Checker roles can be provided for Bulk Upload facility.

5.	Total No. of employees for the year 2019-20 and 2020-21 Domestic employees: Overseas Employees: On contractual basis:	2019-20 • Domestic : 58822 • Overseas : 57 • Contract Employee : 7804 The details of 2020-21 cannot be arrived at this point of time.
6.	Exposures related to electronic banking transactions of Syndicate Bank will be covered or not?	Yes, please refer to the gazette notification CG-DL-E-04032020-216535 published on 04-03-2020 at www.egazette.nic.in
7.	Do you provide any outsourced services to other companies or organizations? Provide details	No
8.	Existing user IDs of both banks will be operated by which entity and will new user IDs be issued?	The amalgamation of the Internet Banking platform is dependent on merger on Core Banking System. The process flow for user registration and access shall be chalked out after CBS migration.
9.	Will both banks use a uniform/ common IT infrastructure?	Canara Bank and Syndicate Bank use i-flex CBS platform.
SECURITY MEASURES		
1.	List of preventive measures installed by Canara Bank	• FAQs & Phishing alerts are furnished as a part of customer education/awareness in the Canara Bank website Net Banking Log in Page. • EFRM solution is integrated with alternate channels like IB, MB, UPI. Velocity check and monitoring of suspicious transactions is implemented for UPI, MB and Internet Banking transactions. The solution is having capabilities of adaptive authentication. • Captcha has been enabled in Net Banking as an additional security measure. • Temporary On / Off for Cards in Mobile Bank / M Serve applications /

केनरा बैंक CANARA BANK Internet & Payment Gateway Section D.B.S. Wing, H.O., Bengaluru - 560 001

		Canara Saathi App (for credit cards) • Canara Bank has implemented the Second Factor authorization for all Online (Card Not present) transactions as a Risk mitigation measure • Device binding for Mobile Banking. Fresh registration is required on change of Mobile sets / SIM even on number portability to prevent fraud through duplicate SIM • Blocking of card on three wrong attempts of PIN • Alert message for debit card transaction providing facility to block the card in case of suspect transactions • Periodical Educative SMS for not sharing Card credentials & Pin and also for frequent change of PIN besides giving this clause in user guide
2.	List of Internal controls and procedures set out	• Anti-Skimming Devices has been installed in all our CAPEX / OPEX ATMs as per RBI Control measures • Up gradation of Windows XP completed in all our CAPEX / OPEX ATMs as per RBI Control Measures • EMV Compliant ATMs implemented • EMV card migration to prevent skimming Anti Skimming devices at ATMs • Introduction of OTP (One Time Password) for Cash withdrawal above Rs. 10000/- in a day by Canara Bank Debit Card holders in Canara Bank ATMs • Fall Back transactions stopped at ATMs • Card less cash withdrawal facility authenticated through OTP to promote contact less ATM transactions to prevent skimming
3.	Details of Internal Audit Department (if any) No. of people employed: Internal Audit Plan Cycle: Any branch subjected to internal audit during last cycle:	No. of people employed: 585 Internal Audit Plan Cycle: varies in the range of 6 months to 18 months basing on the risk rating of the branch Any branch subjected to internal audit during last cycle: All branches are subjected to internal audit based on the risk rating as per point No.2

4.	Physical security available at all premises at all times & during transit	Physical security is available at most of the branches of Canara Bank.
ELECTRONIC & DATA SECURITY		
1.	Total Number of Data Processing Centres	2
2.	Physical security features at data processing centres	There are multi-level access card required to enter the premises. There are multiple level of certificates namely: Quality management: ISO/IEC 9001:2015 Service management: ISO/IEC 20000-1:2011 ISMS - ISO/IEC 27001:2013
3.	Are there any positive entry control procedures used to restrict the entry of non-authorized personnel	Yes
4.	Are passwords used to afford varying levels of entry to the computer system depending on the need and authorization of the user	Yes
5.	Does the system enforce regular password change	Yes
6.	Is the use of terminals restricted only to authorized personnel	Yes
7.	Are employees allowed to access computer systems from home terminals?	No
8.	How does the bank prevent unauthorized access to client's/investor's main processing systems?	Systems are protected by multiple levels of firewalls, WAF and SIEM.

Date: 05-03-2020

Place: Bangalore

Deputy General Manager

ए.वी.वी. सत्यनारायणा मूर्ति
उप महा प्रबंधक
A.V.V. SATYANARAYANA MURTHY
DEPUTY GENERAL MANAGER
ह.अ.सं. / S. P. No. 29999