भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

Confidential

RBI/2016-17/
DBS.CO/CSITE/BC.4226 /31.01.015/2016-17 November 25, 2016

To
The Chairman/ Managing Director /Chief Executive Officer
All Scheduled Commercial Banks (excluding Regional Rural Banks)

Madam / Dear Sir,

Cyber Security Controls – frauds related to trade finance transactions – misuse of SWIFT

It has been reported that certain transactions involving fraudulent Letters of Credit / Comfort were transmitted using the SWIFT messaging system. In this connection, attention is invited to our circular DBS.CO/CSITE/BC.4/33.01.01/2016-17 dated August 3, 2016 on Cyber Security Controls – SWIFT, wherein indicative list of best practices to strengthen the security environment for SWIFT usage had been provided. Banks had also been advised to introduce additional checks, as required, for addressing specific issues inherent to their business environment. Banks may also refer to our letter DBS.CO.CFMC.No1379/23.08.003/2016-17 dated August 10, 2016 and accompanying Caution Advice No. 4094 on Fraud – Letter of Comfort – Buyers Credit – Misuse of SWIFT messaging system.

2. With the objective of analysing certain operational procedures in respect of trade finance transactions, a questionnaire on practices followed by banks while using SWIFT infrastructure was forwarded to select banks. Based on the responses submitted by the banks, several common deficiencies were discernible, which are listed below:

(a) Several banks followed a decentralised setup for SWIFT operations, which entailed multiple SWIFT nodes at various branches and significantly high number of users (in some cases, number of users was in excess of one thousand). The existence of such high number of user IDs increased the probability of compromise of credentials, which in turn exposed the bank to heightened risk of fraudulent activities as well as potential malware attacks.

(b) Several banks did not have robust oversight on SWIFT operations, even under decentralised setup. There was no/little audit oversight on the SWIFT framework,

बैंकिंग पर्यवेक्षण विभाग, केंद्रीय कार्यालय, वर्ल्ड ट्रेड सेंटर, सेंटर- I, कफ परेड, कोलाबा, मुंबई -400005
Department of Banking Supervision, Central Office, World Trade Centre, Cuffe Parade, Colaba, Mumbai 400005
टेलीफ़ोन/ Tele: +91 22 22189131-39; फैक्स / Fax +91 22 22180157; ईमेल /email : cgmicdbsco@rbi.org.in

despite significant financial ramifications. Although administration of SWIFT was delegated to junior level officers and the financial powers exercised by such officials was much above those delegated to similar level officials at branches or in other operational areas, commensurate oversight was lacking.

(c) In several banks, excessive dependence on vendors for all matters related to SWIFT was observed. Reliance on the vendor was observed even for simple activities such as generation of list of authorised SWIFT users.

(d) Most of the banks did not have straight through processing from CBS for trade finance transactions such as Letters of Credit/Comfort etc. This ability to initiate LC messages without reflection of transaction in the CBS posed serious inherent risk. Despite having a decentralised set-up for SWIFT operations, there was no mechanism to verify whether every outward trade finance related SWIFT message had a corresponding underlying LC and thereby identifying fraudulent LC related SWIFT messages, if any.

3. Banks had not attempted to reconcile SWIFT messages issued for trade finance with the outstanding for payment on due date, thus missing out any anomalies arising out of fraudulent transactions.

4. In view of the aforementioned concerns, banks are advised to initiate, with the approval of their respective Boards, the following steps as applicable to their respective business model:

(a) To verify all SWIFT messages pertaining to documentary credit/trade finance (particularly LCs), say from January 1, 2015 onwards, to ensure that all such transactions are captured in the books of accounts and are supported by genuine underlying transactions. Banks may complete this exercise by February 28, 2017 and report the results to CSITE Cell, DBS, CO by March 15, 2017.

(b) To institute appropriate control framework to ensure that SWIFT messages pertaining to documentary credit/ trade finance are transmitted only after accounting for the transactions in their books / CBS / accounting software.

(c) To strengthen the control framework in respect of all outward SWIFT messages pertaining to documentary credit/trade finance by introducing reconciliation of such messages through concurrent audit.

(d) Banks with decentralised setups could examine whether centralising the approval of SWIFT messages at HO could be a practical solution for creating an

additional layer of security as such a step would immediately create functional separation between maker and approver. Banks could also consider centralising all messages, which are created directly in SWIFT systems both for generation and approval.

(e) To explore Straight Through Processing between CBS and SWIFT messaging system so as to avoid potential fraudulent messages.

5. It may be added that the suggestions made above are illustrative only and further safeguards may need to be implemented appropriately on the use of SWIFT framework, workflow design and business profile of the bank.

6. Please acknowledge receipt.

Yours sincerely,

(R Ravikumar)
Chief General Manager