The lowdown on SWIFT and bank fraud

The Rs. 11,500 crore fraud in the Punjab National Bank where fund transfer through an inter-bank messaging system was not reported to the core banking solution, followed by the cyberattack on the City Union Bank, has put the spotlight once again on SWIFT or the Society for Worldwide Interbank Financial Telecommunication. In February 2016, in the Bangladesh Bank heist, $81 million was fraudulently withdrawn from the central bank of the country, at the Federal Reserve Bank of New York through the SWIFT network. The SWIFT is a secure financial message carrier — in other words, it transports messages from one bank to its intended bank recipient. Its core role is to provide a secure transmission channel so that Bank A knows that its message to Bank B goes to Bank B and no one else. Bank B, in turn, knows that Bank A, and no one other than Bank A, sent, read or altered the message en route. Banks, of course, need to have checks in place before actually sending messages.

The SWIFT is a global member-owned cooperative that is headquartered in Brussels, Belgium. It was founded in 1973 by a group of 239 banks from 15 countries which formed a co-operative utility to develop a secure electronic messaging service and common standards to facilitate cross-border payments. It carries an average of approximately 26 million financial messages each day. In order to use its messaging services, customers need to connect to the SWIFT environment. There are several ways of connecting to it: directly through permanent leased lines, the Internet, or SWIFT's cloud service (Lite2); or indirectly through appointed partners. Messages sent by SWIFT's customers are authenticated using its specialised security and identification technology. Encryption is added as the messages leave the customer environment and enter the SWIFT Environment. Messages remain in the protected SWIFT environment, subject to all its confidentiality and integrity commitments, throughout the transmission process while they are transmitted to the operating centres (OPCs) where they are processed — until they are safely delivered to the receiver.

While all customers are responsible for protecting their own environments, SWIFT established the customer security programme (CSP) in early 2016 to support customers in the fight against a growing cyberthreat.

It is critical that customers prioritise the security network. Last April, SWIFT published a detailed description of the mandatory and advisory customer security controls. This framework describes a set of controls for its customers to implement on their local infrastructure.

So, have Indian banks adopted the best practices to keep the network safe? The best practices should be applied not only to the SWIFT infrastructure within banks, but the full end-to-end transaction ecosystem within their firms, including payments, securities trade and treasury. In the PNB case, one of its biggest failures was the missing link between SWIFT and the bank's backend software. This allowed fraudulent use of a key credit instrument — letters of understanding or a loan request to another bank through the SWIFT network — to transfer funds.

After the fraud, PNB adopted strict SWIFT controls. It has created a separate unit to reauthorise most messages sent over SWIFT by branches. Many other banks are expected to fast-track the integration between SWIFT and their backend systems. To strengthen internal controls, the RBI has set April 30 as an "outer limit" for all public sector banks to integrate SWIFT with core banking solutions. As for SWIFT, a spokesperson said: "First, there is no indication that SWIFT's own network or core messaging services have ever been compromised. SWIFT cannot comment on particular incidents. However, it continues to share insights into modus operandi and indicators of compromise with its customers."

Manojit Saha

END