# LEVERAGE BPM FOR SAFE AND TRANSPARENT BANKING

**By Virender Jeet,** Senior Vice President, Sales & Marketing / Products, Newgen Software

The recent scam in a large public sector bank has revealed how vulnerable the banking sector can be to frauds despite well defined systems and controls. Human intervention in a single one off integration touch point in the complete chain of process can lead to a large scale loss to a bank for a considerable period of time, if undetected.

### But is this a one-off case?

No. Any bank can be a victim. More so with banks that has disjointed processes. In fact, an evolving digital eco system presents challenges to bankers today, specifically in customer verification and make them susceptible to frauds. Business users have to struggle with broken processes to work on disjointed applications which lead to manual intervention and duplicate data for verification


Virender Jeet

during transactions. Operation risk controls around processes therefore, need to be flexible to the changing digital paradigm to avoid such scenarios.

## Why Banks & FIs are vulnerable?

Two strong reasons emerge-

- It is observed that bankers monitor and supervise only funded exposures while processes related to transfers remain opaque as happened. The focus should be on implementing monitoring, control and audit in cases of transfers as well.
- Banks and financial institutions are at the forefront in implementing the latest technology to extend great customer experience. One problem with these so called digital technologies, is that every piece of technology or solution added to a stack creates yet another ivory tower to manage. If not well connected, operational silos are created. For instance, the Core Banking System (CBS) was not linked to SWIFT as in this case. Some employees were authorized to manually carry out the SWIFT transactions and records of the necessary details in the Core Banking System (CBS) were not maintained. This was possible as both the systems were not integrated. Hence, no flags or alarms were ever raised.

Hence, technology, or rather- the lack of the right one to unify of all this together can make banks and FIs vulnerable. Re-defining internal controls leveraging technology can work as protective gears for banks.

## Scam-proofing banks & FIs with Digital Platforms

A logical question surfaces- how can banks avoid such frauds?

There is a strong need to have a robust process automation framework to interface with all peripheral systems and bring them into a single unified framework which is mandatory to commit any transaction. Digital platforms such as BPM can help banks here. BPM enables banks and FIs to centralize and initiate all transactions from basic housekeeping, accounting, auditing, and reporting. With BPM, all the systems, processes, people and things get connected. It is a robust unification platform that knits together day-to-day retail, corporate, financial inclusion software and modules. Bankers receive daily dashboards with discrepancies instantly flagged and visible for easy audit. Monitoring, control, checks and balances are easily put in place with a configurable unified platform that is BPM. Business rules in processes also reduce human intervention to a large extent and a scenario such as this is never created. Another key benefit of BPM is its ability to integrate legacy applications in banks and embrace new-age technologies of mobility, digi sensing, RPA etcto enhance customer experience

> Business users have to struggle with broken processes to work on disjointed applications which lead to manual intervention and duplicate data for verification during transactions

In a nutshell, BPM extends safe, transparent and secure banking by curtailing corporate scams with better monitoring and control. Seamlessly integrated centralized operations coupled with the power of STP is the need of the hour. CR