

# MAJOR INDIAN BANK IMPLEMENTS DATA CENTRIC SECURITY AND MEETS PCI DSS COMPLIANCE

One of the largest banks in India that serves over hundreds of millions of customers across thousands of locations has adopted data centric security. The company operates extensively with PANs—personal account numbers—as well as other types of personal data for their financial operations and organizational objectives. Much of this information is deemed sensitive according to PCI DSS and requires adequate data protection. Without proper security, this major financial services company was at risk of non-compliance which could have resulted in numerous financial and legal consequences.

## CHALLENGES

With more than 100 million customers, this financial services company continually strives to best serve its clients and customer base. However, it faces a challenge of understanding trends, patterns, and insights of its diverse clientele. To overcome this challenge, analysis of client data is imperative to gaining insights for strategic business decision-making. The bank faced a problem, however, in that much of the data used for analysis—PANs, customer names, track2 characters—was deemed sensitive under PCI DSS (Payment Card Industry Data Security Standards) which is enforced for all financial institutions by the Reserve Bank of India.

The financial services company operates across various data environments which falls under PCI scope. BASE24, provided by ACI Worldwide, is a popular payment switch which the bank uses for OLTP (Online Transaction Processing). In addition, this company also uses Golden Gate, a data replication solution created by Oracle, for their production environment. For these applications, the Reserve Bank of India mandates that transaction log files, POS transaction log files, host interface log files, customer authorization files, host interface store and forward files, and ATM log files comply with PCI DSS. The key issue, however, was the company's use of filing systems that contained primary account numbers, credit card numbers and other financial information with specific bank identification details that posed challenges to meeting regulatory compliance standards.

"Working with comforte and implementation of their data security solution greatly enhanced our organization. With their tokenization, we were able to improve our security posture and concurrently solve challenges for PCI compliance. Going forward, our organization has the right protection technology in place to most effectively manage sensitive information and boost our security initiatives" – Chief Manager, Major Indian Public Sector Bank.

## BUSINESS OBJECTIVES

- ▶ Achieve PCI compliance
- ▶ Protect cardholder data
- ▶ Enhance security initiatives

## SECURE YOUR GROWTH WITH COMFORTE

With more than 20 years of experience in data protection on truly mission-critical systems, comforte is the perfect partner for organizations who want to protect their most valuable asset: data. Comforte's Data Protection Suite, SecurDPS, has been built from the ground up to best address data security in a world that is driven by digital business innovations, empowered customers, and continuous technology disruptions. We are here to help secure your growth by providing expertise, an innovative technology suite, and local support.

To learn more, get in touch with a comforte representative today by visiting: [comforte.com/contact](https://comforte.com/contact)



## SOLUTIONS

In order to overcome these challenges with sensitive data, this financial services company needed a data security solution with desired features like format preserving tokenization, remote file support, comprehensive key management, granular access control and auditing, and seamless interaction with disaster recovery solutions to best protect the personal information for PCI compliance. Therefore, they chose comforte SecurDPS Nonstop to solve this challenge. Comforte was able to transparently integrate into their BASE24 application without requiring changes in source code and the implementation was completed within 2 months without a disruption to strategic operations. Using this method, comforte was then able to tokenize all PANs, customer names, track2 characters, and other sensitive data which greatly assisted in mitigating noncompliance risks. This also allowed their stakeholders responsible for data-driven processes and decision-making to carry on operations as normal.

## BENEFITS

With the adoption of SecurDPS Nonstop, this bank has achieved substantial improvements to their HPE Nonstop system by successfully tokenizing sensitive data. By achieving PCI certification, they were able to avoid financial penalties of fines up to \$500,000 per incident and other perpetrated fraud losses with the primary account numbers in the event of a compromise or data breach. In securing the trust of their customers through the protection of personal information, the financial services company also has a strong foundation for continued growth and expansion. Moving forward, the company can adequately protect primary account numbers, customer names, track2 characters and other sensitive data elements that arise in their BASE24 and Golden Gate applications while still meeting compliance mandates.



*Working with comforte and implementation of their data security solution greatly enhanced our organization. With their tokenization, we were able to improve our security posture and concurrently solve challenges for PCI compliance. Going forward, our organization has the right protection technology in place to most effectively manage sensitive information and boost our security initiative.*

*Chief Manager, Major Indian Public Sector Bank*

