VERDICT

News

SmartStream gets PCI-DSS certification

By Mohamed Dabo July 29, 2020

SmartStream Technologies, the financial Transaction Lifecycle Management (TLM®) solutions provider, has received certification for PCI-DSS version 3.2.1, level 1 (the highest level).

The PCI certification ensures the security of card data at businesses through a set of requirements established by the PCI Security Standards Council (PCI SSC).

The PCI Security Standards Council (PCI SSC) is a global forum that brings together payments industry stakeholders to develop and drive adoption of data security standards and resources for safe payments worldwide.

PCI security requirements include a number of commonly known best practices, such as: Installation of firewalls. Encryption of data transmissions. Use of anti-virus software.

PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data.

“The process was rigorous”

In order to achieve the PCI-DSS version 3.2.1, level 1 certification, SmartStream had to demonstrating high levels of security across the whole organisation.

This involved such areas as physical security, personnel security, fraud control mechanisms, IT & data security and data privacy – on a fully monitored business environment.

“The process was rigorous, it included revisiting numerous policies, testing security solutions and implementing new processes, it was a collaborative team effort across all of the business units,” SmartStream CEO Haytham Kaddoura.

SmartStream’s reconciliations platform and OnDemand (SaaS) services using its flagship solutions: TLM Reconciliations, TLM Aurora and SmartStream Air (Artificial Intelligence Reconciliations), have been certified at the highest level of security standards.

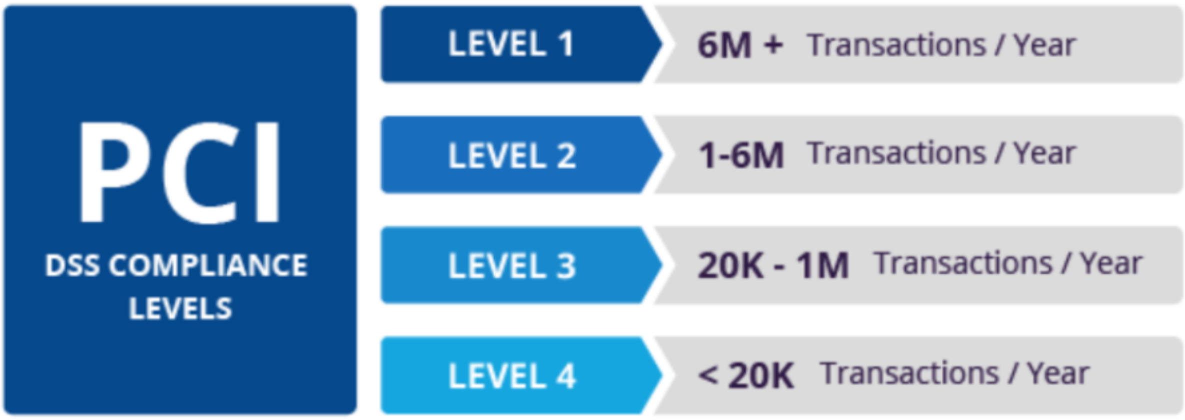
This also includes the departments, staff, locations and processes which supports the complete service model.

“This requirement was driven by our clients and it is now critical and demanded by all financial institutions. It simply gives us the hallmark of trust, which is especially important in these current times, with data security and fraud detection being so high on the corporate agenda,” Kaddoura said.

PCI DSS Compliance levels

PCI compliance is divided into four levels, based on the annual number of credit or debit card transactions that a business processes.

The classification level determines what an enterprise needs to do to remain compliant.



PCI

DSS COMPLIANCE LEVELS

LEVEL 1 — 6M + Transactions / Year

LEVEL 2 — 1-6M Transactions / Year

LEVEL 3 — 20K - 1M Transactions / Year

LEVEL 4 — < 20K Transactions / Year

Source: PCI

- **Level 1**: Applies to merchants processing more than six million real-world credit or debit card transactions annually. Conducted by an authorized PCI auditor, they must undergo an internal audit once a year. In addition, once a quarter they must submit to a PCI scan by an Approved Scanning Vendor (ASV).
- **Level 2**: Applies to merchants processing between one and six million real-world credit or debit card transactions annually. They're required to complete an assessment once a year using a Self-Assessment Questionnaire (SAQ). Additionally, a quarterly PCI scan may be required.
- **Level 3**: Applies to merchants processing between 20,000 and one million e-commerce transactions annually. They must complete a yearly assessment using the relevant SAQ. A quarterly PCI scan may also be required.
- **Level 4**: Applies to merchants processing fewer than 20,000 e-commerce transactions annually, or those that process up to one million real-world transactions. A yearly assessment using the relevant SAQ must be completed and a quarterly PCI scan may be required.