Three years on from Bangladesh

Tackling fraud with SWIFT Payment Controls

Your top FAQs answered

Why would my institution need Payment Controls?

Fraudsters are finding various methods of how to send fraudulent messages from back offices and over the SWIFT network. Payment Controls allows clients to build rules which can prevent or alert certain anomalous or higher risk payments.

What is **Payment Controls**?

- Zero footprint, in-network payment monitoring
- Alert or block suspicious payments in real-time

What features does **Payment Controls** offer?

- Correspondent banking focused models
- Highly subscriber-configurable
- Alert Management & workflow
- Payment release/abort
- Activity & risk reporting

What are the benefits of **Payment Controls**?

- Secondary control of payment traffic, separate from your own infrastructure
- Block fraudulent payments before they happen
- Rules configured based upon each institution's own traffic
- Leverages SWIFT & the community's knowledge and experience

Why has SWIFT developed this tool?

SWIFT's position as within the industry means that we have two important roles to play.

- The information SWIFT has about the developing nature of the threat allows us to develop sophisticated and targeted tools to combating the bad actors. Ensuring that even with limited expertise in the cyber domain you are able to protect yourself.

- SWIFT's infrastructure allows us to provide these tools in a highly cost efficient way.

What does Payment Controls screen?

It screens your sent MT 103, 202, 202cov messages.

What kind of rules can I build in Payment Controls?

The Rules available within Payment Controls are very flexible, but also under contestant development to ensure they are able to tackle the agile and sophisticated bad actors. They include things such as business calendars, where we look at non-business days and normal business hours, value or volume thresholds for country, currency, single entity or group combinations, or New Institutions to identify institutions you haven't sent transactions to before.

How easily can the tool be set up?

Payment Controls is very easy to set up. It only takes a few weeks, and we support you through the whole process. As part of the set up SWIFT supports you through the iterative process of testing and tuning your rules, similar to other Fraud or AML systems.

Who should be involved in this process from my bank?

Similar to other compliance tools it is the Compliance Operations teams who deal with the alerts, and the Fraud Compliance and Information Security Team who build and maintain the tools.

Is there any physical hardware I need to install?

No, only physical USB tokens are required. There is no change required to your SWIFT connection, the messages are screened as they pass over the SWIFT network.

www.swift.com