SWIFT Payment Controls
Fact sheet

Protect your payment operations against fraudulent attacks

Features

- Real-time, 'in-flight' monitoring of the payments you send
- Secure, SWIFT-hosted service with zero-footprint and instant switch-on
- Complete independence from your internal back-office systems
- Intelligent technology learns behavioural patterns over time, supporting continuous improvement

Benefits

- Stop high-risk payments in real time
- Improve payment speed, transparency and reliability
- Provide business assurance to counterparties
- Mitigate regulatory and reputational risk

The nature and impact of fraud in the financial services industry has changed. Cyber-criminals are now targeting their attacks at the very heart of the institution, gaining control of the back-office and fraudulently sending payment instructions over the SWIFT network in an attempt to steal from the institution's internal accounts. They try to conceal their actions by deleting transaction records, complicating the recovery of stolen funds.

Successfully preventing such attacks is hard work. Banks need to monitor payments in real time and instantly take action if a transaction seems risky. This may demand the payment be blocked, awaiting review. In addition, it is essential to have accurate payment reporting, independent of in-house systems. For smaller institutions with limited resources, it's critical that such tools are easy to implement, simple to use, and affordable.

SWIFT Payment Controls

combines real-time monitoring, alerting and blocking of sent payments, with daily reporting. It helps institutions detect and prevent high risk payments and mitigates business disruption and financial losses in the event of back-office compromise.

SWIFT Payment Controls

helps mitigate fraud risk through its unique alerting and reporting capabilities.

Alerting

Payment Controls provides real-time alerting on your outbound messages. Validated, correspondent-focused models and indicators can be aligned with your risk policies and operational processes.

You can manage settings based on message type, by country, by institution or in various combinations of these criteria. Rules can be edited and deployed instantaneously by the subscriber, at any time, and tested against live payment flows. The flexible, intuitive user interface makes it easy to fine-tune settings as policies and risks evolve.

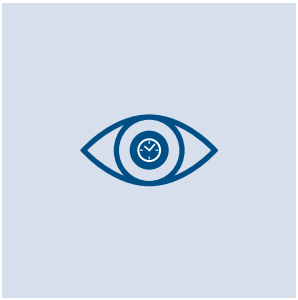
Reporting

Payment Controls provides an independent record of your inbound and outbound payment activity, enabling you to validate whether your in-house payment system's record of activity is correct.

The reports cover your previous day's payment activities, helping you validate activity and assess risk. Transaction value and volume totals are compared to daily value and volume averages over the previous 24 months, helping you identify and understand significant changes. You can pinpoint unusual activity, as well as identifying new beneficiary relationships and out-of-hours transactions.

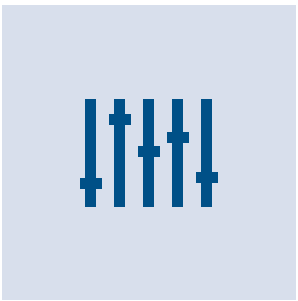
Manage risk policy to identify uncharacteristic payments

Payment Controls monitors the payments you send, and can block these in real-time if necessary to prevent fraud. High-risk and out-of-policy payments are alerted instantly, enabling you to act quickly to prevent losses.



Define stronger policy to protect your operations

By understanding the patterns of payments you send over time, you can develop more effective and robust controls. Monitoring rules can be deployed in real time to enforce policies and protect payment operations. Doing this reduces the risk of fraud and gives operations teams tighter overall control.



Validate payment messages against SWIFT's network record

Robust business monitoring and reconciliation capabilities let you validate your internal records against SWIFT's secure record of your payments. Payment Controls helps identify unusual payment behaviours, even if hackers have tampered with systems, database and log files.

Building a safer, more secure future
SWIFT is committed to developing new services to reduce the threat of cyber-attack and fraud, and to strengthen areas of potential weakness in your payment processing. Payment Controls is an important part of SWIFT's Customer Security Programme, a community-driven initiative that is enhancing cyber security for the global financial industry.

Alerting

Threshold
Payments that are high risk or fall outside of business policy, based upon individual payment value or aggregate value/volume

Profiles
Payment behaviour that is uncharacteristic, based on past learned behaviour

New scenarios
Payments sent through or to new institutions, in new currencies or using previously unseen message types

Account monitoring
Payments to/from high-risk beneficiary/originator customer accounts or payments to/from accounts that are not present on a subscriber-defined 'accept list'

Risk Scoring
A single risk score provided on your transactions through an intelligent, self-learning algorithm tuned by SWIFT to the changing cyber threat characteristics.

Badly formed messages[1]
Payments that are preceded by elevated/repetitive NACKs to the same beneficiary customer account

Alert-only mode
The triggering payment message will be delivered to your receiver, without interruption, and an alert will be generated simultaneously. You can investigate this alert and undertake any necessary response and recovery activities.

Manual review mode
The triggering payment message will be held in-network by the service and an alert will be generated for your review and investigation. You decide whether to abort the message or release it for delivery.

Email notification
Get instantaneously notified via email of the occurrence of key events (e.g. a message being blocked by an alert).

Reporting

Validate activity
Quickly assess and validate inbound and outbound payment flows. Daily activity is aggregated by message type, currency, country and counterparty, enabling easy comparison with internal reports from core systems. Daily value and transaction references help you match individual transactions for more detailed validation.

Assess risk
Highlight large or unusual message flows that may indicate fraud risks. You can review new or unfamiliar counterparties or counterparty combinations, including nested activity. Transactions sent or received outside of user-defined business hours are highlighted.

Message coverage

Payment Controls covers MT 103, MT 202, MT 202COV, and soon pacs.004, pacs.008 and pacs.009 as the industry moves to ISO20022. For alerting this is for sent payments. For reporting this is for both sent and received payments.

57505 - February 2021