Financial Crime Compliance

SWIFT Payment Controls

Protecting your payment operations
against fraudulent attacks

Making it easy for you to mitigate fraudulent attacks…

With SWIFT Payment Controls, you can protect your institution against fraudulent attacks.

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.

…by detecting and preventing high risk payments, as well as supporting recovery

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.

Manage risk policy to identify uncharacteristic payments

Payment Controls monitors the payments you send and can block these in real time 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, the system allows you to 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 your systems, database and log files.

Combining real-time monitoring, alerting and blocking of sent payments...

SWIFT Payment Controls helps mitigate fraud risk through its unique alerting and reporting capabilities for payment operations.

Alerting

Payment Controls offers validated, correspondent-focused models and indicators. You choose how you use these, aligned with your risks and operational processes. Its flexible, easy-to-use interface supports fine-tuning as policies and risks evolve.

Rule types include:

Business calendars: Payments sent on non-business days or outside of normal business hours.

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’.

Badly formed messages*: Payments that are preceded by elevated/repetitive NACKs to the same beneficiary customer account.

You have freedom to easily configure monitoring rules that focus on and align to your risks. You can differentiate policy by your sending role (originator vs. intermediary), by message type, by country, by institution or in various combinations of these. You can easily control your accepted behaviour as well as contextualise your monitoring based upon past payment activities. Rules can be edited and deployed instantaneously by the subscriber, at any time. Rules can be tested against live payment flows.

Payment Controls will alert you when any payment triggers a rule. You can configure any rule in one of three operational modes:

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.

Auto-action mode*: The triggering payment message will be automatically aborted and an alert will be generated simultaneously.

You may also choose to be notified by email if any payment triggers a rule.

* Future enhancements

...with independent daily reporting

Reporting

Payment Controls reporting 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.

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.

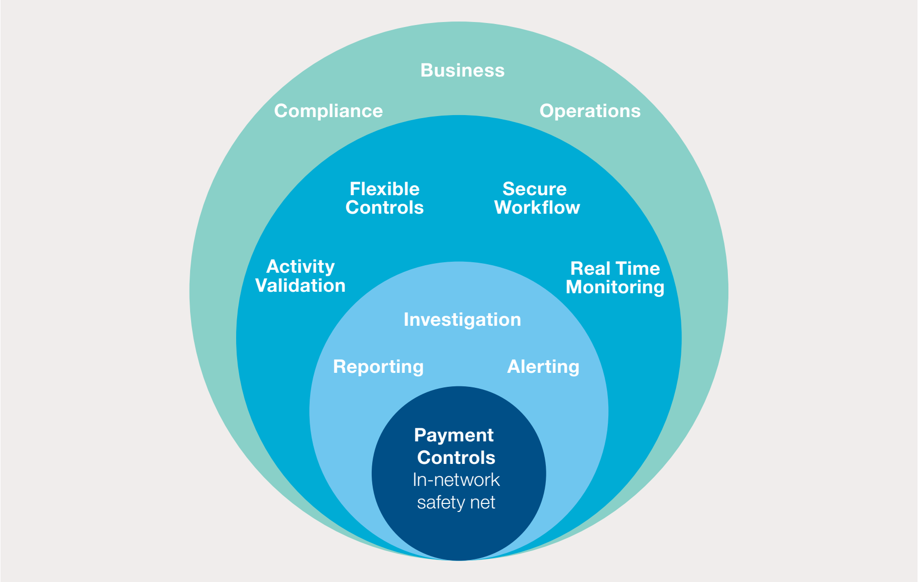
Mitigating fraud risk…

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

Features

- Real-time, 'in-flight' monitoring of the payments you send
- Intelligent technology that learns behavioural patterns over time, supporting continuous improvement
- Secure, SWIFT-hosted service with zero footprint and instant switch-on
- Powerful but simple to use pre-built reports covering both sent and received payments, easily tailored by subscribers
- Simple rule configuration management with mix and match alert operating modes
- Secure, audited workflow to streamline investigations and manage blocked payments

Capabilities

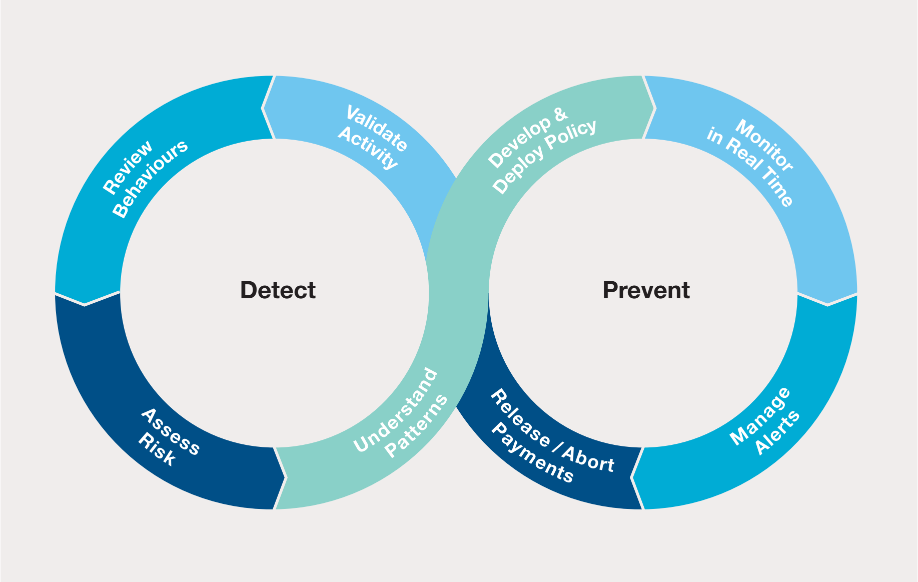


…building a safer, more secure future

Benefits

- Stop high-risk payments in real-time
- Mitigate regulatory and reputational risk
- Improve payment speed, transparency and reliability
- Complete independence from your internal back-office systems
- Provide business assurance to counterparties
- Alert coverage of key payment messages MT103, MT202, MT202COV, MT205 and MT205COV

Process flow



About SWIFT

SWIFT is a global member owned cooperative and the world's leading provider of secure financial messaging services. We provide our community with a platform for messaging and standards for communicating, and we offer products and services to facilitate access and integration, identification, analysis and regulatory compliance.

Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories. While SWIFT does not hold funds or manage accounts on behalf of customers, we enable our global community of users to communicate securely, exchanging standardised financial messages in a reliable way, thereby supporting global and local financial flows, as well as trade and commerce all around the world.

As their trusted provider, we relentlessly pursue operational excellence; we support our community in addressing cyber threats; and we continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. Our products and services support our community's access and integration, business intelligence, reference data and financial crime compliance needs. SWIFT also brings the financial community together – at global, regional and local levels – to shape market practice, define standards and debate issues of mutual interest or concern.

Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.

For more information, visit

Web:	www.swift.com
Twitter:	@swiftcommunity
LinkedIn:	SWIFT

August 2018, 57377