

How to detect and intercept payment anomalies in real-time

Features



Rules-based and scoring-based approaches: implement controls that are easy to configure and rapid to deploy



Swift network-wide insights: account-level statistics from the entire Swift network, highlighting anomalies that FIs do not have a view on individually



Hosted on the Swift network: a separation from your back-office systems that is crucial in the event of a cyberattack or operational issue



Intelligent technologies: Payment Controls learn behavioural patterns over time to support continuous improvement of efficiency and effectiveness

Benefits



Alert or block payment anomalies in real-time, before they are released from the Swift network



Improve payment speed and reduce friction by detecting anomalies before payments are released



Reduce operational costs of recall and recovery, and mitigate regulatory and reputational risks related to fraud



Provide business assurance to your counterparties on your control environment

Payment Controls (PCS) can help you to detect payment anomalies that are indicative of fraud affecting your institution, customers, and counterparties, or cause operational issues.

How it works

Payment Controls screen your outgoing Swift payment messages against rules you've made based on your risk appetite, business needs, and payments policies. Alerting and blocking take place in real time, so you can intercept suspicious messages before they are released, preventing financial loss and reputational damage.

Payment Controls screens all of your outgoing FIN and ISO 20022 messages, including MT103, MT202, MT202cov, pacs008, pacs009, and pacs004. And, from 2023 Payment Controls will also leverage pseudonymised account information which has been shared by the Swift community to help users address additional risk scenarios at the customer and account levels.

Fraud affecting your institution



Payments fraud targeting your institution typically involves attacks performed by external parties on your payments infrastructure by installing malware, either remotely or by using the institution's staff. Fraudsters can also resort to social engineering techniques such as phishing or impersonation of legitimate entities, to manipulate employees into authorising a payment on behalf of your FI.

As a Swift-hosted control separate from your institution's infrastructure, Payment Controls provides your safety net within the Swift network to alert or block payments presenting anomalies for your institution, based on your rules configuration, payments policy, risk appetite and past traffic patterns.

Fraud affecting your customers



Fraud targeting Financial Institutions' customers and counterparties is a pressing issue, with regulators and law enforcement agencies across the world warning banks and their customers of the growing threats of impersonation, social engineering and phishing attempts. Some regulators have reached the stage of proposing regulatory updates, including imposing refunds or additional mandatory controls at the transaction level.

To that end, Payment Controls can complement your existing controls by providing unique account-level insights from the entire Swift network. Originating institutions can be warned if their customer is about to initiate a payment presenting anomalies at the network level and leverage this information in their anomaly detection processes in order to potentially avoid the indirect costs linked to the recovery of fraudulent funds.

Operational issues



Operational issues can arise whether you have fully automated, semi-automated or fully manual controls in place. These can lead to institutions processing or initiating payments containing errors, or to sending payments by mistake altogether – leading to operational costs for recall, recovery, or refunds as well as reputational and regulatory risks.

Some operational issues present anomalies that Payment Controls can help you to detect before your payments are released from the Swift network, including payments sent to/ from the wrong ordering or beneficiary account, payments in the wrong amount or wrong currency, or repeated payments.



Alert or block outliers

Each rule for anomaly detection can be set in ‘blocking’ or ‘non-blocking mode’. In non-blocking mode, the outgoing message will be sent over the Swift network, and you will receive an alert. In blocking mode, the outgoing message will be held until you make a ‘2-eye’ or ‘4-eye’ decision to release or abort the message.



Institution level rules

Institution-level rules can be used to detect uncharacteristic outgoing activity, based on the institutions involved in a payment transaction. You can define these rules based on individual payments (e.g. amount, destination, time the message was sent), or on your past traffic patterns (e.g. new payment corridors or aggregate value and volumes). The service includes a Risk Scoring rule, which can be used as an additional control.



Account level rules

Detect anomalies at the account level, based on rules that leverage unique data from the entire Swift network. From the end of 2022, you’ll be able to detect new scenarios and duplicate payments on debtor and creditor accounts. Additionally, you can create ‘forbid’ and ‘allow’ account lists for monitoring, and these rules can, like others, be combined with other rule types.



Combine rules

Payment Controls allow you to easily configure and rapidly deploy flexible rules tailored to your risk appetite and payments policies. These rules can combine to help you manage different scenarios to detect fraudulent or anomalous payments. For example, outside of your business hours, you can choose to block messages that exceed meet a certain condition, against a certain value threshold only.

Flexible controls that are rapid and simple to deploy

Thresholds

Alert or block payments exceeding your defined threshold (absolute or relative value) on a single payment, on an aggregated amount or on aggregated message count. Rules can also apply filters for specific currencies, country corridors and/or FI corridors.

New Scenarios

Alert or block payments sent to or via new corridors (country, institution, BIC8) and/or in new currencies for your institution.

Business Calendar

Alert or block payments sent outside your defined business hours and days.

Risk Scoring

Alert of block payments exceeding your selected risk score, computed against a history of past fraudulent transactions taking place on the Swift network.

Account Monitoring

Alert of block payments sent to accounts figuring on your “forbid” account lists, or allow payments sent to accounts figuring on your “allow” account lists.

New Account Scenario

Alert or block payments from/to new ordering/beneficiary accounts or a new relationship between two known accounts, and/or detect the usage of a new currency by/from/between known or unknown accounts – looking at accounts within your institution or at account analytics from the entire Swift network. Depending on your configuration, you could detect the following scenarios:

- An account in your institution is about to send a payment to a beneficiary account that has never been seen before by your institution or by the Swift network and/or to a beneficiary account that has never used this currency before. This might indicate that your customer account has been hacked or fell victim to a scam, or an operational issue.

- An account in your institution is about to send a payment on the Swift network for the very first time AND/OR in a currency that it has never used before on the Swift network. This might indicate that your customer account has been hacked or fell victim to a scam, or an operational issue.

- An account in your institution is about to send a payment to a beneficiary account it has never exchanged a Swift payment with before and/or in a currency that those two accounts have never used together before. This might indicate an operational issue.

Combination: Alert or block payments that meet the conditions of two or more rules, to target more specific risk scenarios and enhance the effectiveness and efficiency of your alert generation.

Duplicate Payments

Alert or block repeated payments of the same amount and currency to or from a given account within 1 or 24 hours – looking at accounts within your institution or at account analytics from the entire Swift network. Depending on your configuration, you could detect the following scenarios:

- An account in your institution is about to send a payment of the same amount and currency, to different beneficiary accounts within 1 or 24 hours. This might indicate that your customer’s account was hacked or compromised.
- An account in your institution is about to send a payment to a beneficiary account that received a payment of the same amount and currency from another account in another institution, in the past 1 or 24 hours. This might indicate that your customer fell victim to a scam or fraud scheme.
- An account in your institution is about to send a payment of the same amount and currency to the same beneficiary account within 1 or 24 hours. This might be indicative of an operational issue or errors in your institution’s systems.

Rules that are easy to configure, rapid to implement and instinctive to review: Payment Controls provides you with updated Payments Activity Reports, modelling the alert rate that would be generated for different rules according to your parameters and configuration. The Ruleset generator also allows you to simulate the predicted alert rate impact of implementing a rule according to payments you've sent in the past.



Multiple notification channels

Payment Controls enables you to be notified when alerts are generated in the portal, via email and/or SMS notifications.



Flexible organisational and administrative set-up

Payment Controls can cater to your institution's size and structure by providing you with the flexibility you need, including by offering centralised BIC or decentralised BIC governance structures as well as 2-eyes or 4-eyes alert management workflows.



Payment Controls Reporting

Payment Controls Reporting offers daily reporting on your incoming and outgoing payment transactions, based on Swift's independent network reports, allowing rapid reconciliation and risk identification.



Message coverage

Payment Controls cover both FIN and ISO 20022 payment message types: MT 103, MT 202, MT 202COV, and pacs.004, pacs.008 and pacs.009. For alerting this is for sent payments. For reporting this is for both sent and received payments.
