SWIFT Webinar:
Descubra cómo proteger a su institución contra el fraude de pagos

Yugo Musac, Especialista en cumplimiento, **SWIFT**

12 febrero 2019

The attacks on SWIFT customers have all followed the same Modus Operandi

- Attackers are **well-organised and sophisticated**
- There is (still) **no evidence** that SWIFT's network, core messaging services or OPCs have been compromised
- All **Indicator of compromise details** are published on the SWIFT Information Sharing and Analysis Centers (ISAC) portal

Step 1
Attackers compromise customer's environment

- **Malware** injected by e-mail phishing, USB device, rogue URL or insider
- Long **reconnaissance** period monitoring banks' back office processes

Step 2
Attackers obtain valid operator credentials

- Keylogging / screenshot malware looking for **valid account ID and password** credentials

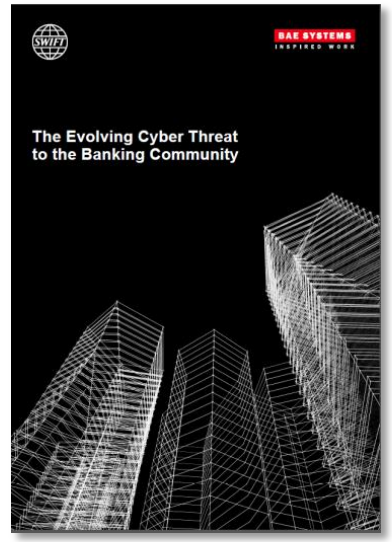
Step 3
Attackers submit fraudulent messages

- Attacker impersonate the operator / approver and submits **fraudulent payment instructions**
- May happen outside the normal bank working hours / over public holiday

Step 4
Attackers hide the evidence

Gain time by:

- Deleting or manipulating records / log used in reconciliation
- Wiping Master Boot Record

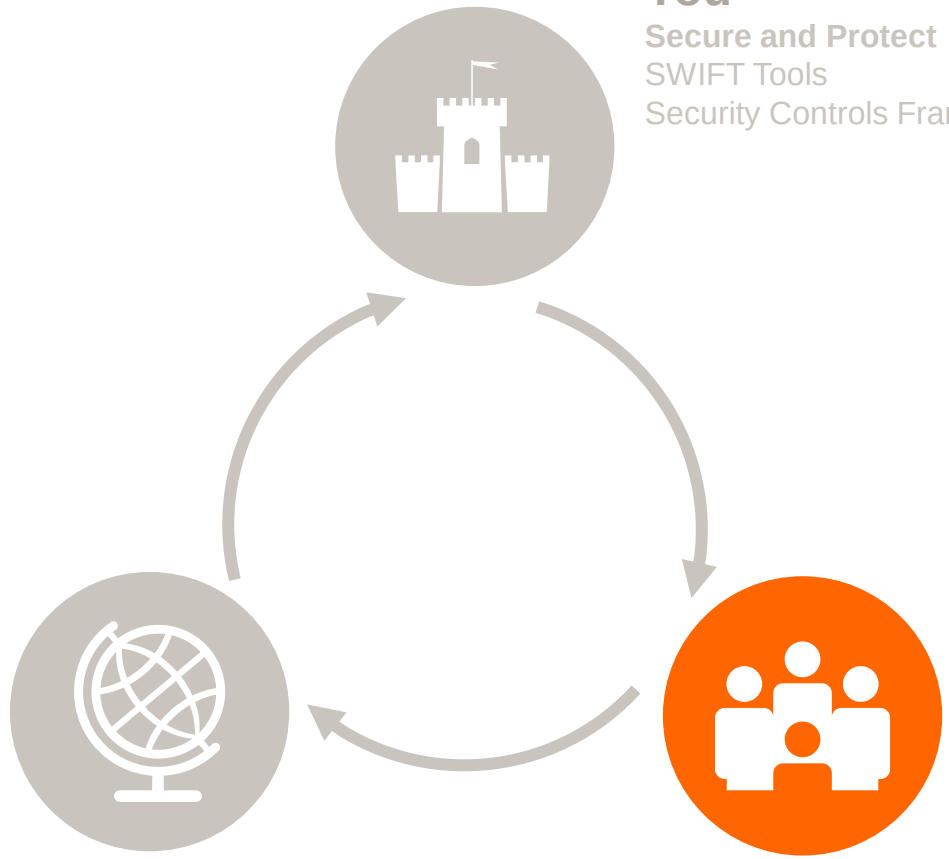


You

Secure and Protect

SWIFT Tools

Security Controls Framework



Your Community

Share and Prepare

Intelligence Sharing

SWIFT ISAC Portal

Your Counterparts

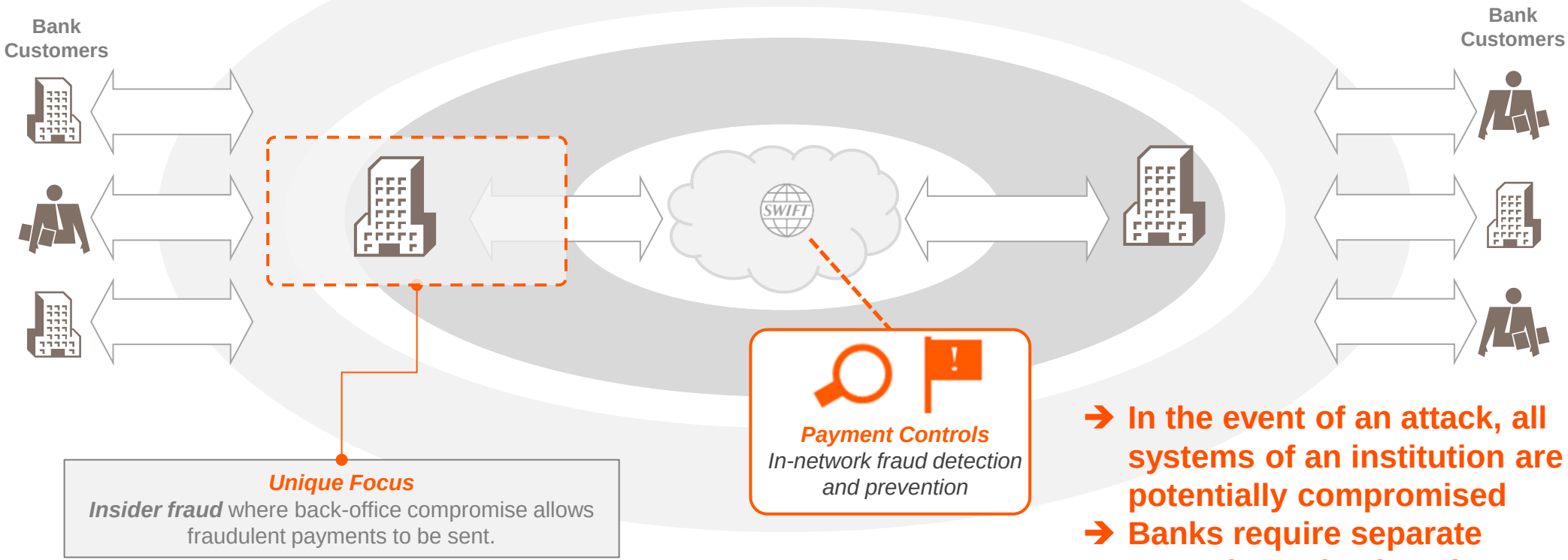
Detect and Prevent

RMA, Daily Validation Reports and Payment Controls

New type of fraud

Fraud is increasingly sophisticated and patterns are changing – moving from data theft to payment fraud

"**Financial institutions and payment infrastructures are the new targets" ***



➔ **In the event of an attack, all systems of an institution are potentially compromised**

➔ **Banks require separate controls to check and stop payments**

* Source: * ***"2017 PAYMENT THREATS AND FRAUD TRENDS REPORT"*** European Payments Council.

SWIFT's Payment Controls

Reduce Fraud Risks	Reduce Reputational Risks	Build Trust

- ✓ **Real-time transaction monitoring** – Proactive fraud prevention tool enables subscribers to identify and stop payments
- ✓ **In-network security** – no reliance on integrity of internal systems, a unique view of your SWIFT payment activity
- ✓ **Sophisticated & flexible rules, based on your real data**– Supporting a safe payment network for all correspondents
- ✓ **Fast incident response** – build and implement rules quickly to respond to new incidents

Payment Controls | A fraud detection & prevention tool

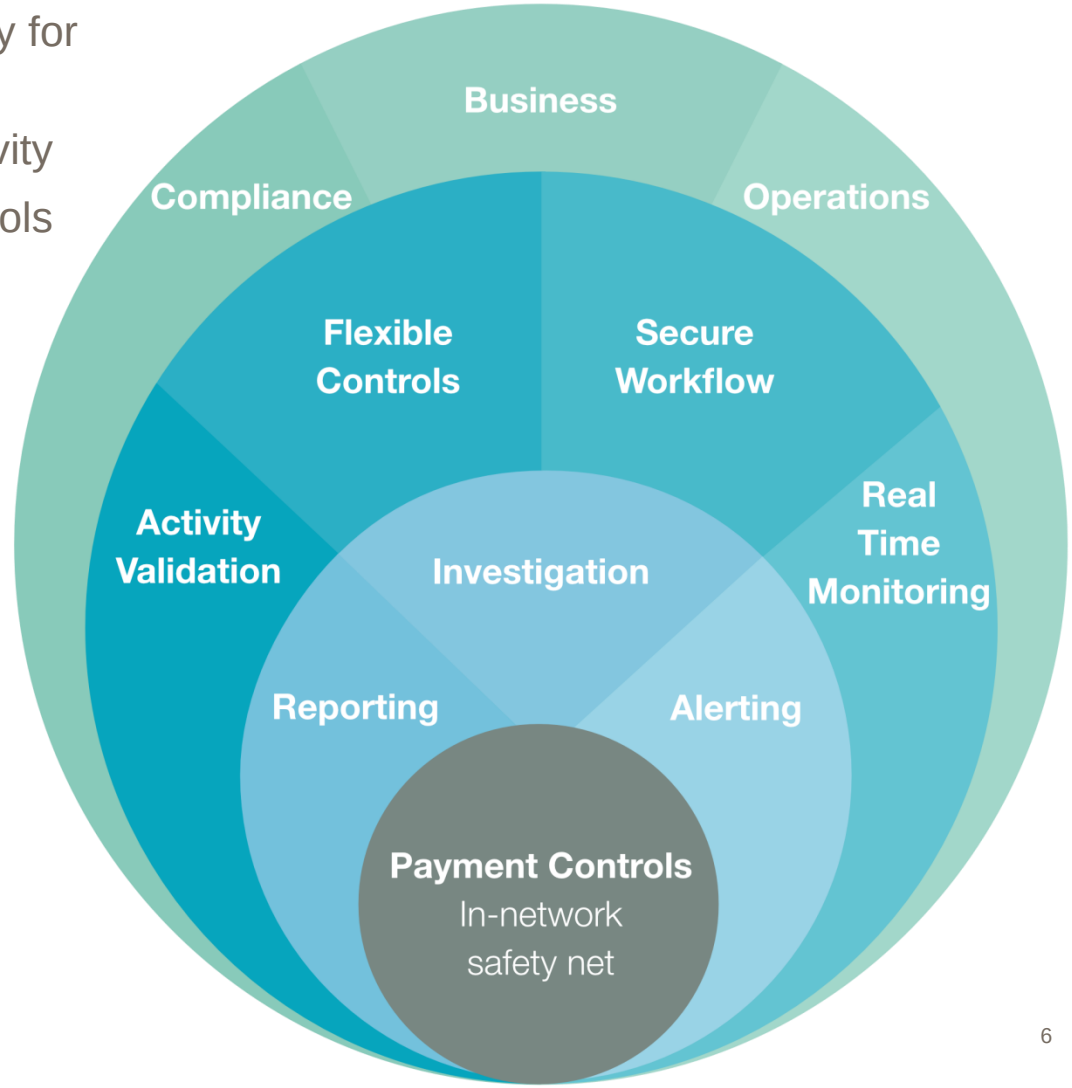
Make **SWIFT's Payment Controls** part of your strategy for protecting yourself against cyber-threats.

- A unique network view of your SWIFT payment activity
- Detect payment risks with ***a***lerting & investigation tools
- Define your own Payment & Risk policy
- Build rules based on your traffic data

Message scope – Initially focused on FIN payment messages: **MT103, MT202, MT202cov,** MT205 & MT205cov

Enables your institution to:

✓ Control your payment processes
✓ Manage risk
✓ Ensure policies are met



Payment Controls

2 Modules

Module 1

Reporting

Activity and Risk reporting
Inbound and Outbound
Group and/or Entity reporting

Available Now

Module 2

Alerting

Real-time alerting/blocking
Outbound
Subscriber-controlled rules

Available Q3 2018

Module 1

Daily activity and risk reporting with Daily Validation Reports

In the event of an attack the accuracy of data in interface systems may be compromised.

Validate Activity

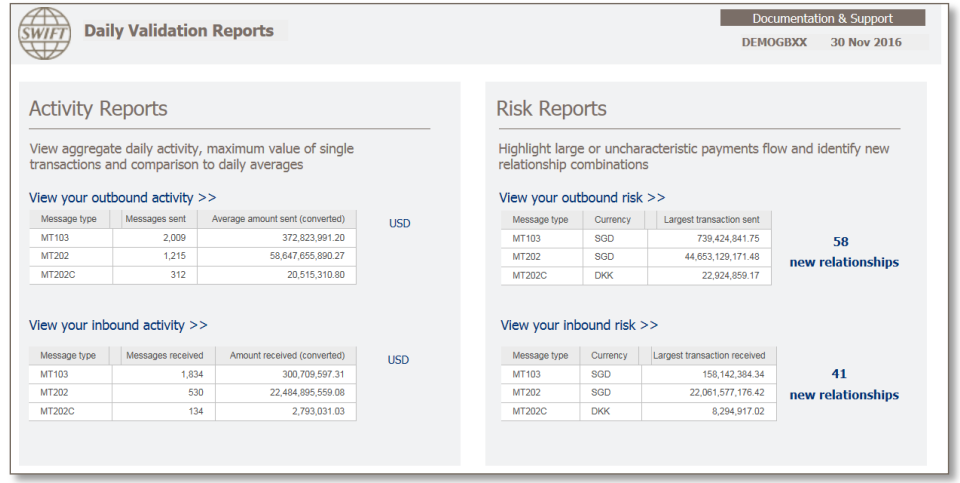
- Validate aggregated daily activity and *transactions* (reference and value) for a Group or a BIC8 across the payment chain
- Daily volume and value totals, maximum value of single transactions and comparisons to *24 months historical profile*

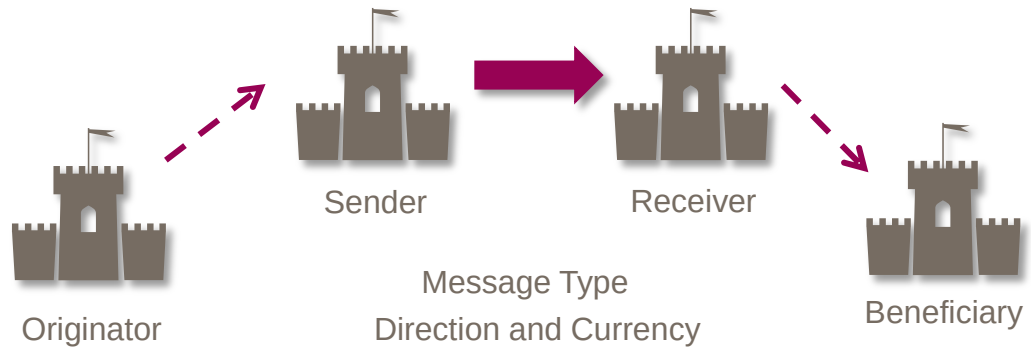
Assess Risks

- Assess large or unusual message flows based on different risk factors (largest transactions, largest aggregates, or deviation with average activity).
- Identifies *new combinations of parties* in payment chain
- highlights transactions sent *outside of business hours*

Review Behaviours

- Ensure alignment to Compliance policy

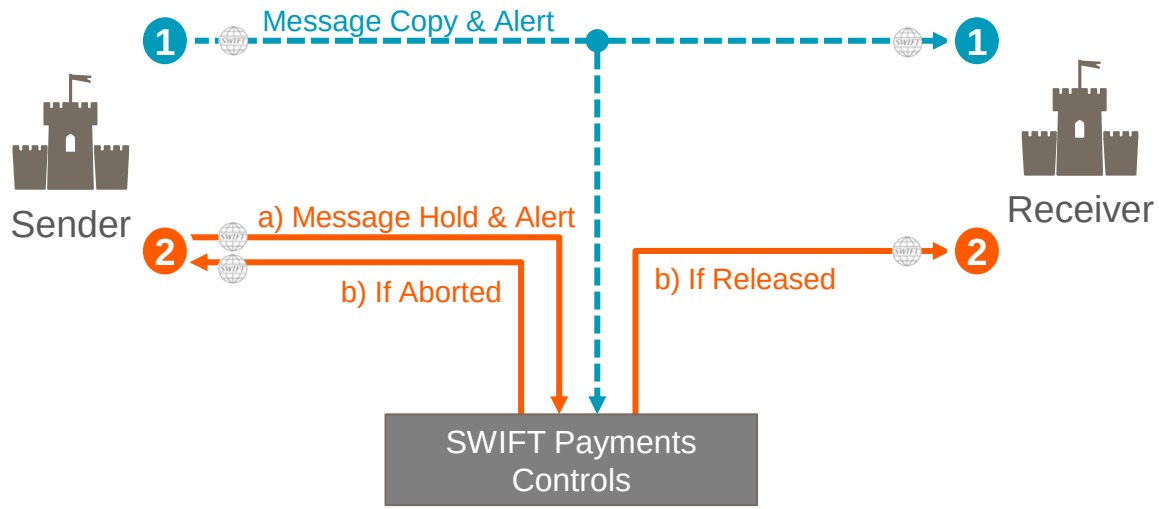




Module 2

Real-time monitoring overview

- **Real-time, in-network monitoring**:
  - **Payment Policy** – encode institution policies & monitor at a network level, e.g. to prevent payments above certain currency thresholds from being conducted without additional review, prevent out-of-hours payments
  - **Risk Policy** – monitor and detect uncharacteristic messaging activity that may be indicative of fraud and review or flag such payments
- Provides a **zero-footprint, secure in-network, payment safety-net** against payment risks
- Flexible **business workflow** and **rule management**
- **Operating modes:** alert-only / alert-hold / auto-action
- Focused on **sender controls**



Module 2

Topics covered by the Rules

Threshold — Protect against individual and aggregated payment behaviour that is a potential fraud risk or falls outside of business policy

Profiling/ Learning — Identify & protect against payment behaviour that is uncharacteristic, based upon past learned behaviour

Business Calendars — Identify payments that are sent on non-business days or outside normal business hours

Suspicious Accounts — Verify end customer account numbers against an institution black list of account numbers believed to be high risk

New Institutions — Identify payments involving individual institutional participants or chains that have not been seen previously, based upon historical message flows

Badly Formed Messages — Identify and stop messages where preceded by repetitive NACKs to the same recipient

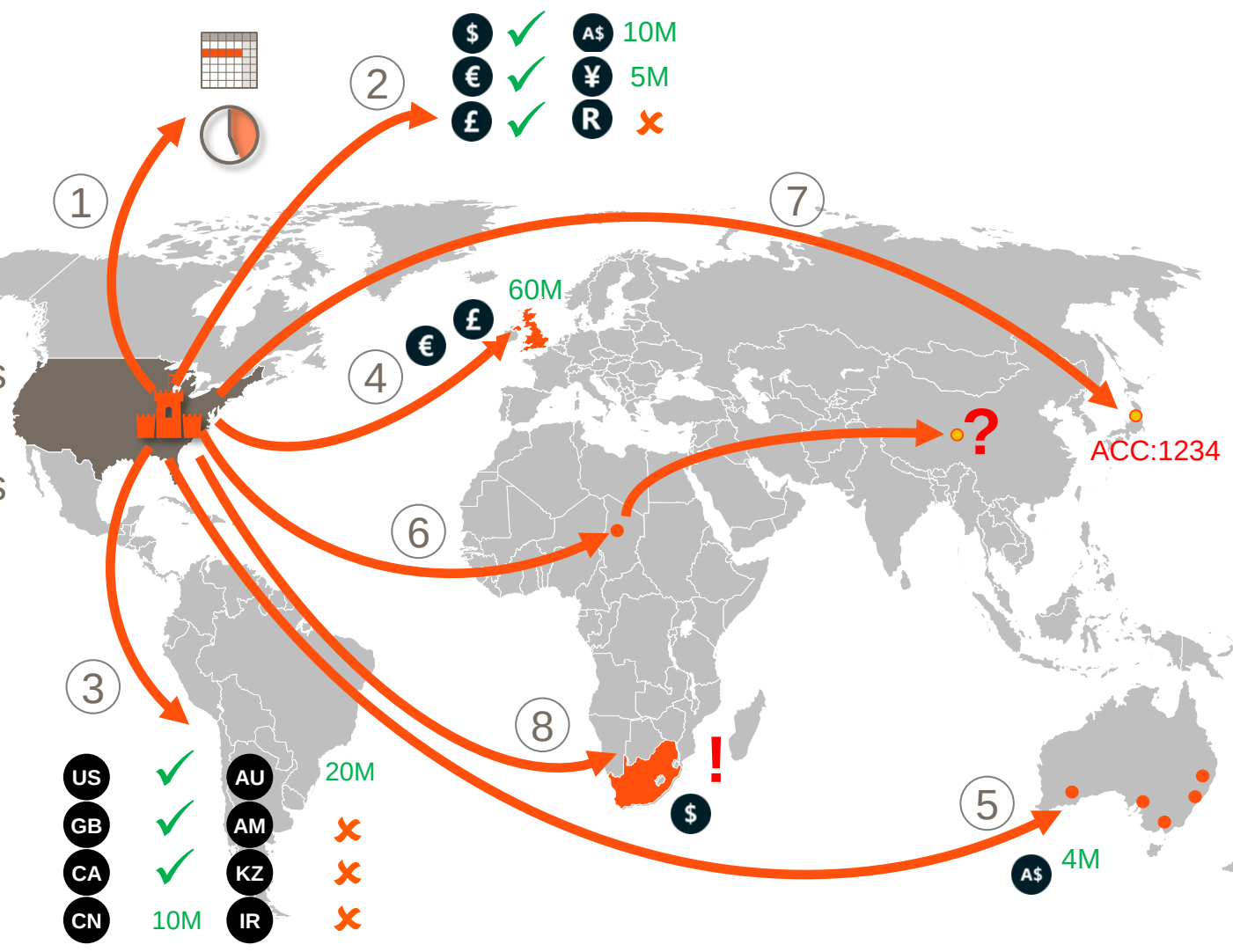
2019

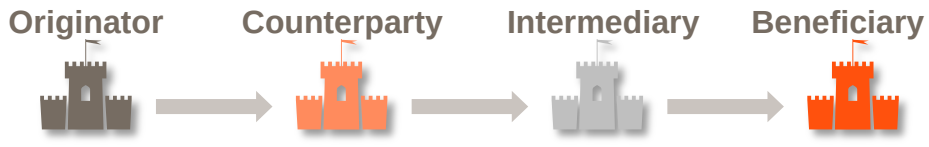
Use Cases

Flexible parameters including:

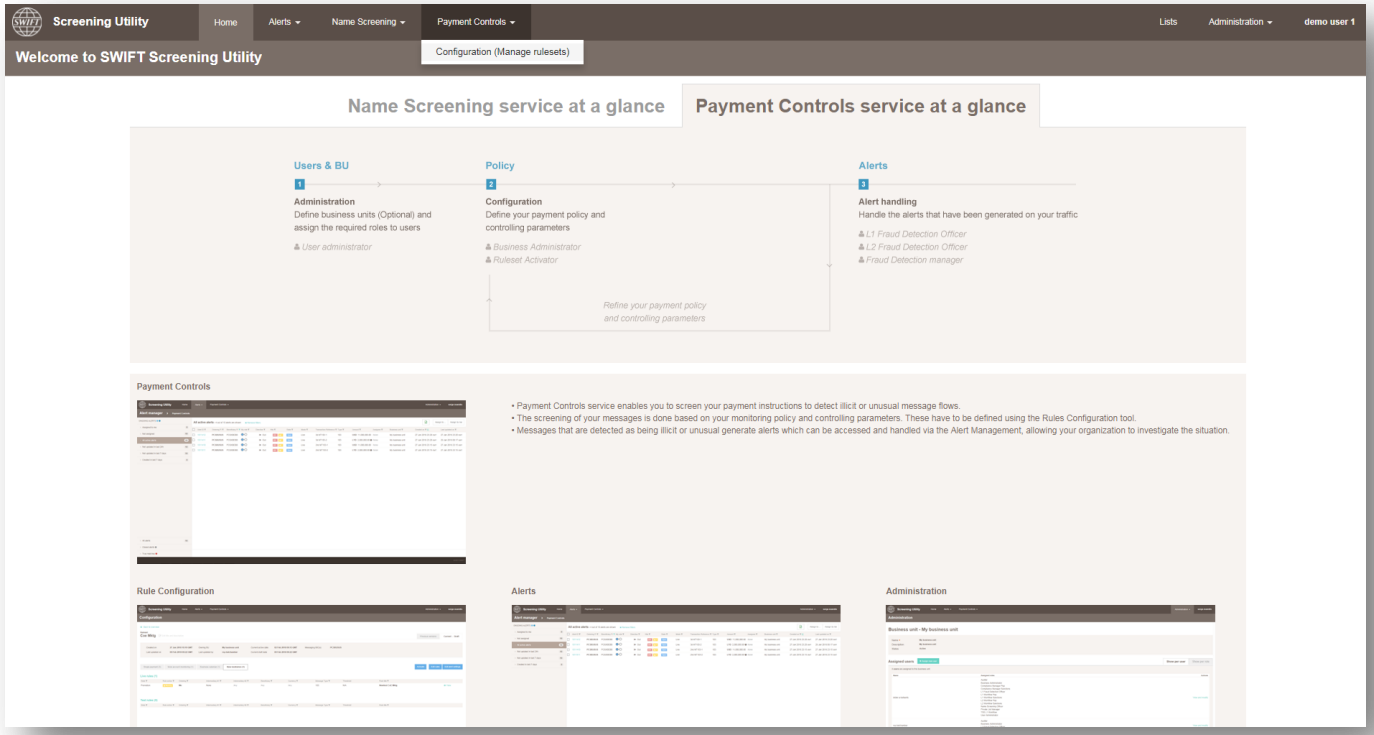
1. Business hours and days
2. Currency whitelist / blacklists, single & aggregate payment limits
3. Country whitelist / blacklists, single & aggregate payment limits
4. Country & currency threshold combinations
5. BIC & Entity institution limits
6. New payment flows
7. Suspicious accounts
8. Uncharacteristic behaviours

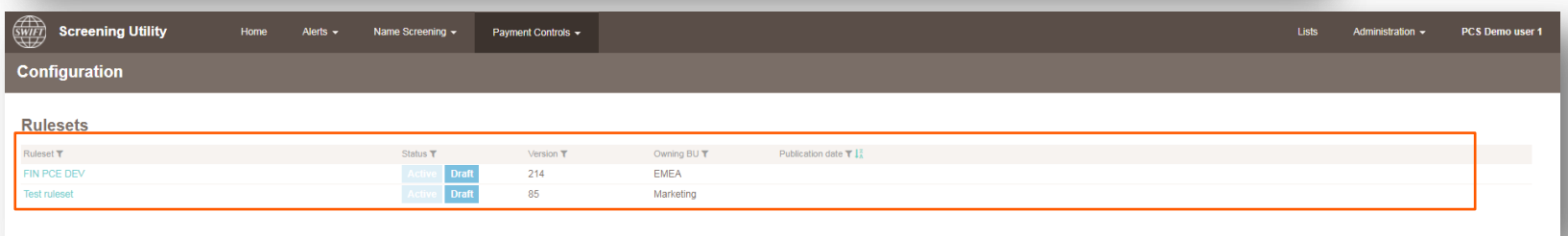
Across the complete payment chain





Payment Controls real-time alerting – Set up of a monitoring policy





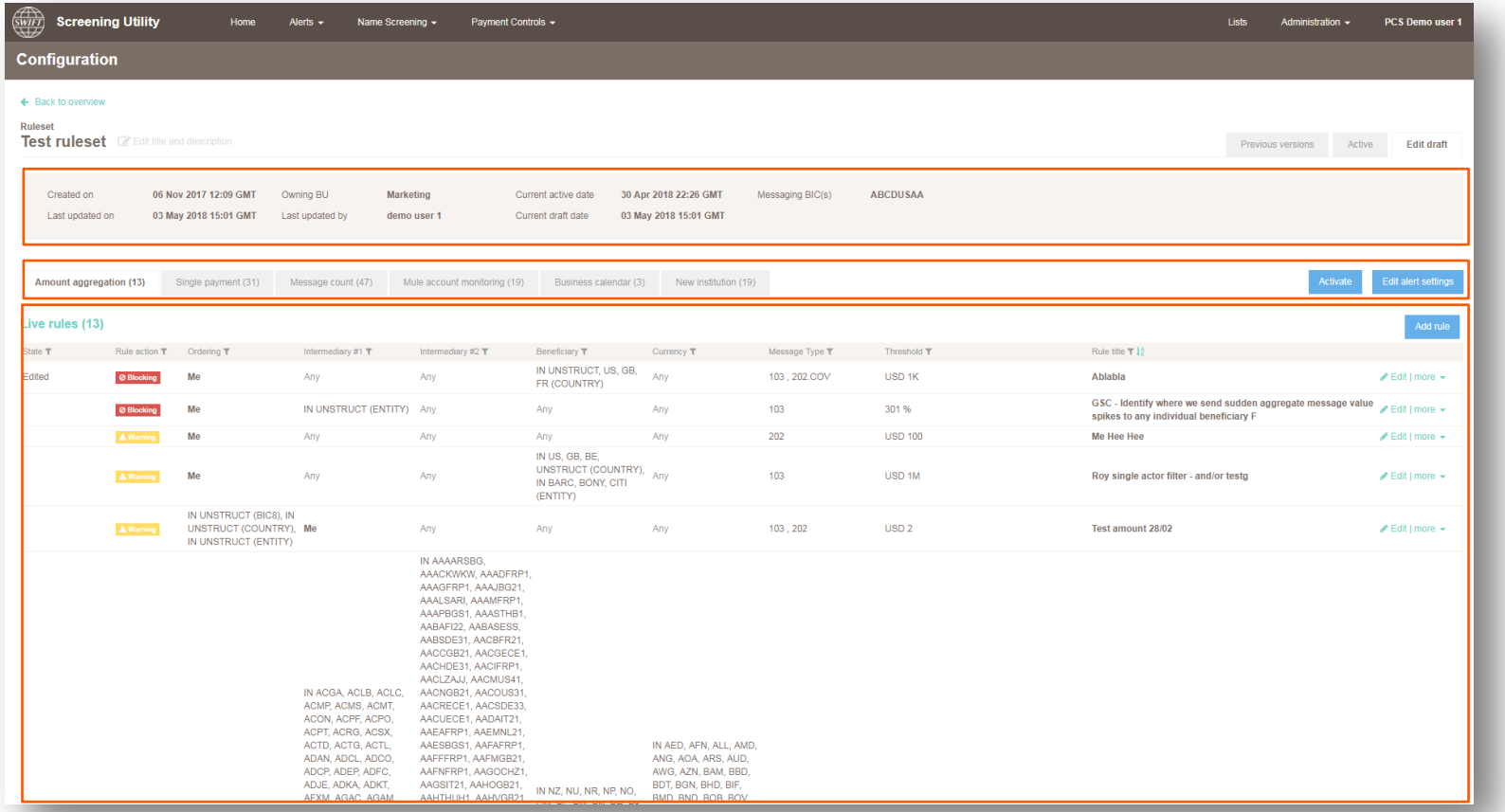
Payment Controls is part of the **Screening Utility platform**, which hosts a number of Financial Crime Compliance services.

Within Payment Controls you will be able to:

- Set up and **manage User & Business Units**
- Create and manage your **Payment Policy**
- **Manage** and **review alerts**

Rulesets allow institutions to encode their payment policy based on multiple sub-rules.

Once a Ruleset is activated the rules are now processed against the message types the subscriber has selected per rule.
A **version history** is kept of each Ruleset that is created/ amended.



A summary view is provided of your Ruleset under each **Rule type**.
Rules can either be in **Live or Test mode**. With Live mode you can choose to block or alert-only. With Test mode you run a proposed rule against live traffic to understand the behaviour of the rule before adding this to your live rules

Each **Ruleset** displays **summary information** on:

- When it was created/ updated and by whom
- Who the owning BU is
- When it was activated and for which BIC(s)

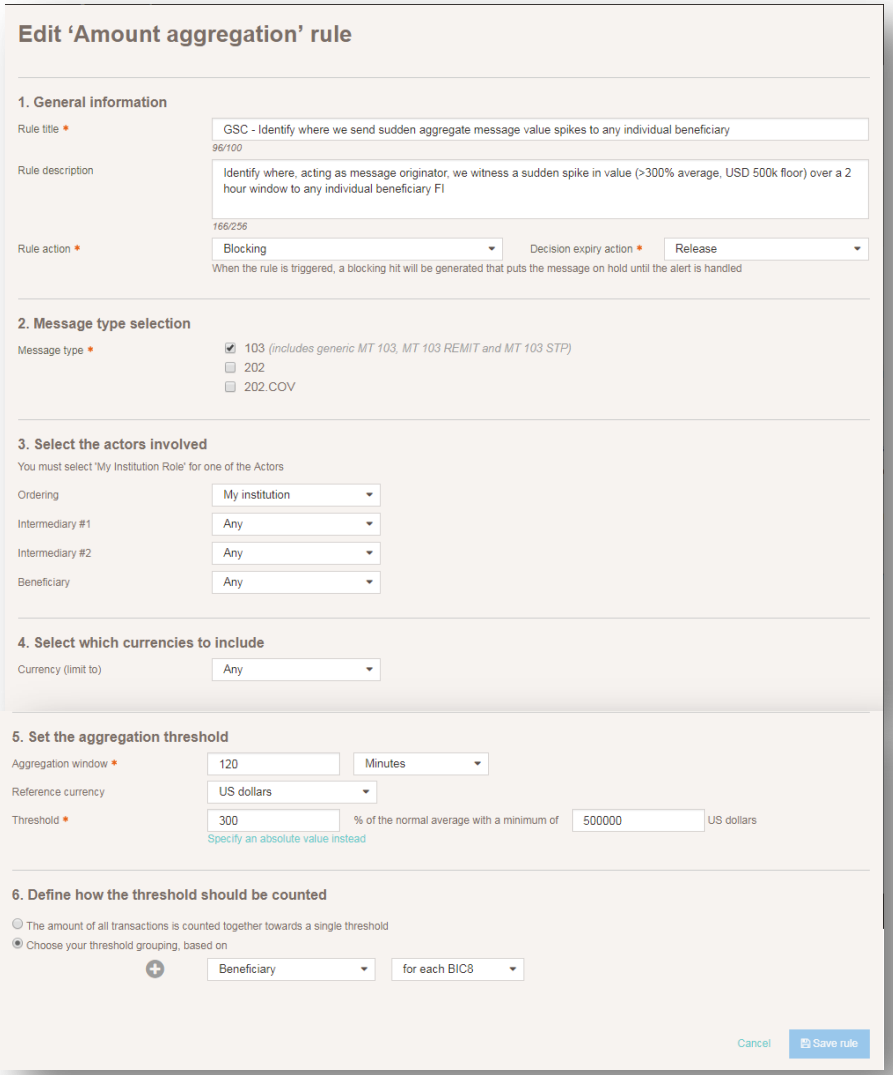
A subscribing customer can choose to set up rules across **Rule types**

Within **Alert settings** a subscriber can choose:

- Various **workflow types**, including 4-eyes
- (Optionally) set **automated abort/release timer** on blocking alerts

With the right permissions a User can:

- Activate a ruleset
- Create/ amend/ delete rules
- Pro-/ demote rules (live or test)



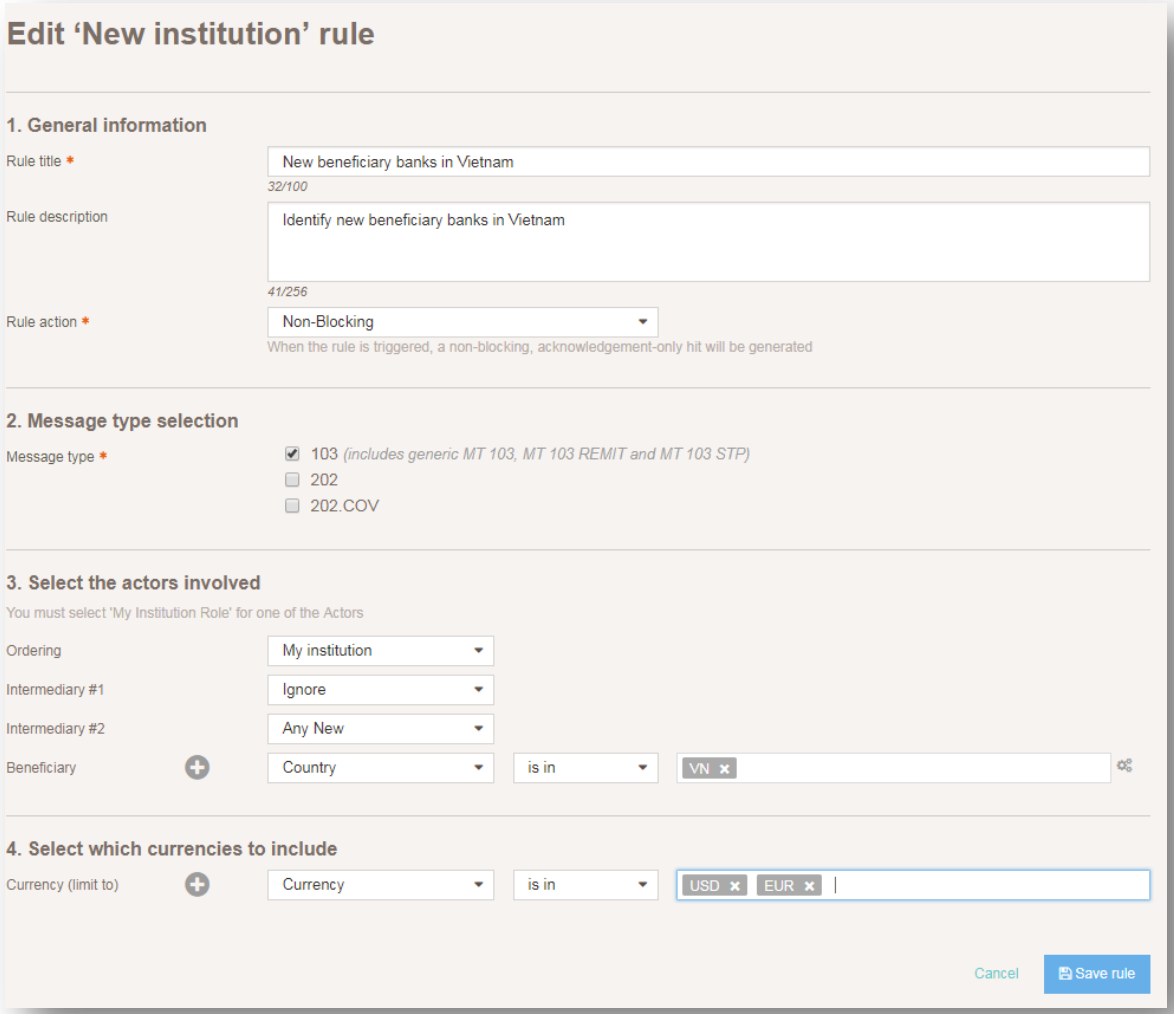
Rules are created using the following step-by-step process:

1. Define title and description
2. Select a rule operational mode: Blocking or non-blocking
3. Select the message types this rule should consider
4. Select the scope of actors (payment roles) to which the rule is applied – define your messaging role as an institution and optionally filter message participants that you wish to monitor
5. Optionally select the currencies involved

Set up a 'Threshold or Amount aggregation' rule

1. Set the aggregation threshold and period (for aggregation window)
2. Define the actor against which the threshold should be applied

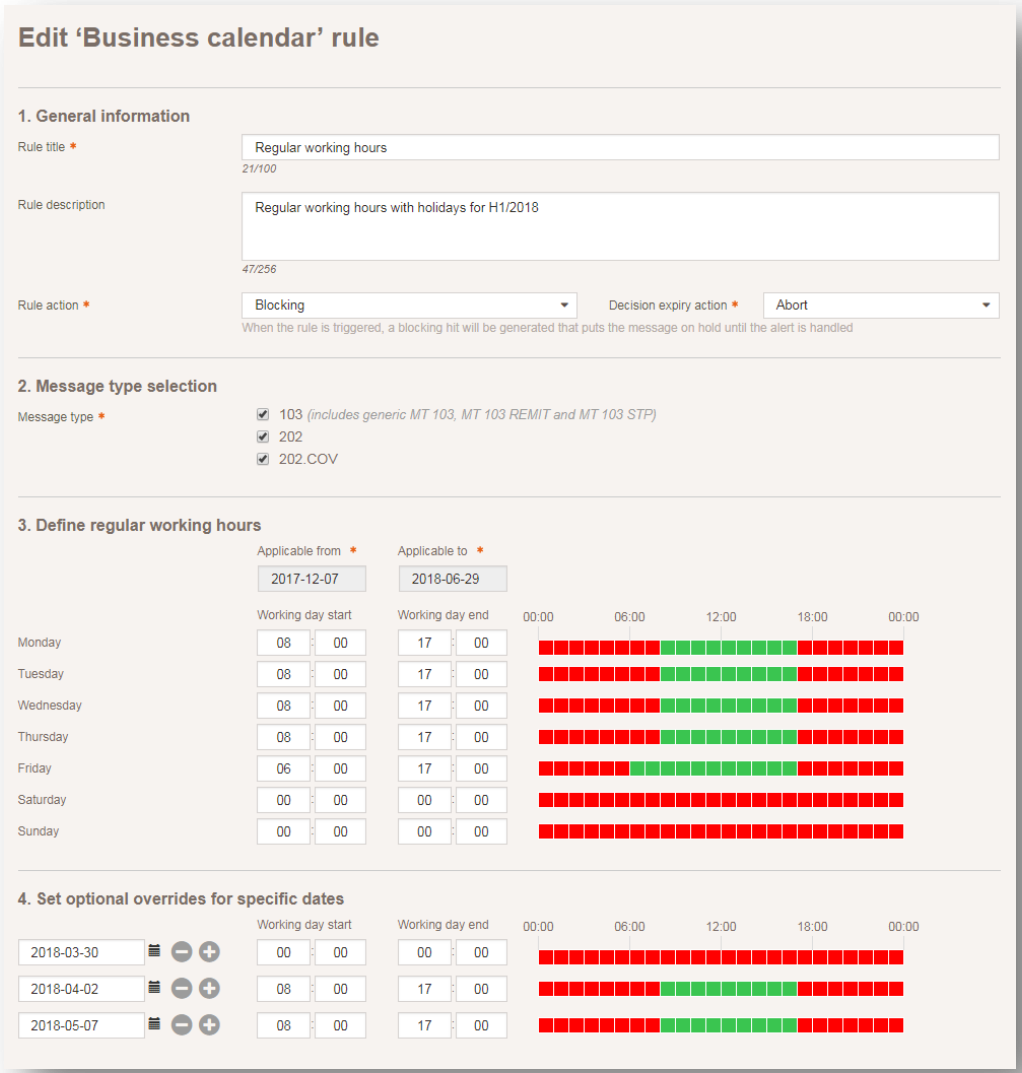
In this example rule alerts where my institution acts as the ordering bank and sends MT103s with aggregate value, calculated over the past 2 hours, more than 3X the normal average. Split this threshold by each individual beneficiary BIC8 we have sent to over this 2 hour period.



Set up a 'New Institution' rule

This rule allows you to identify unusual message flows: by institutional participants, currency and message type.

In this example we are identifying any payment via any new downstream intermediary where the payment goes to a previously unseen beneficiary bank in Vietnam and these payments are in US Dollars and Euros.



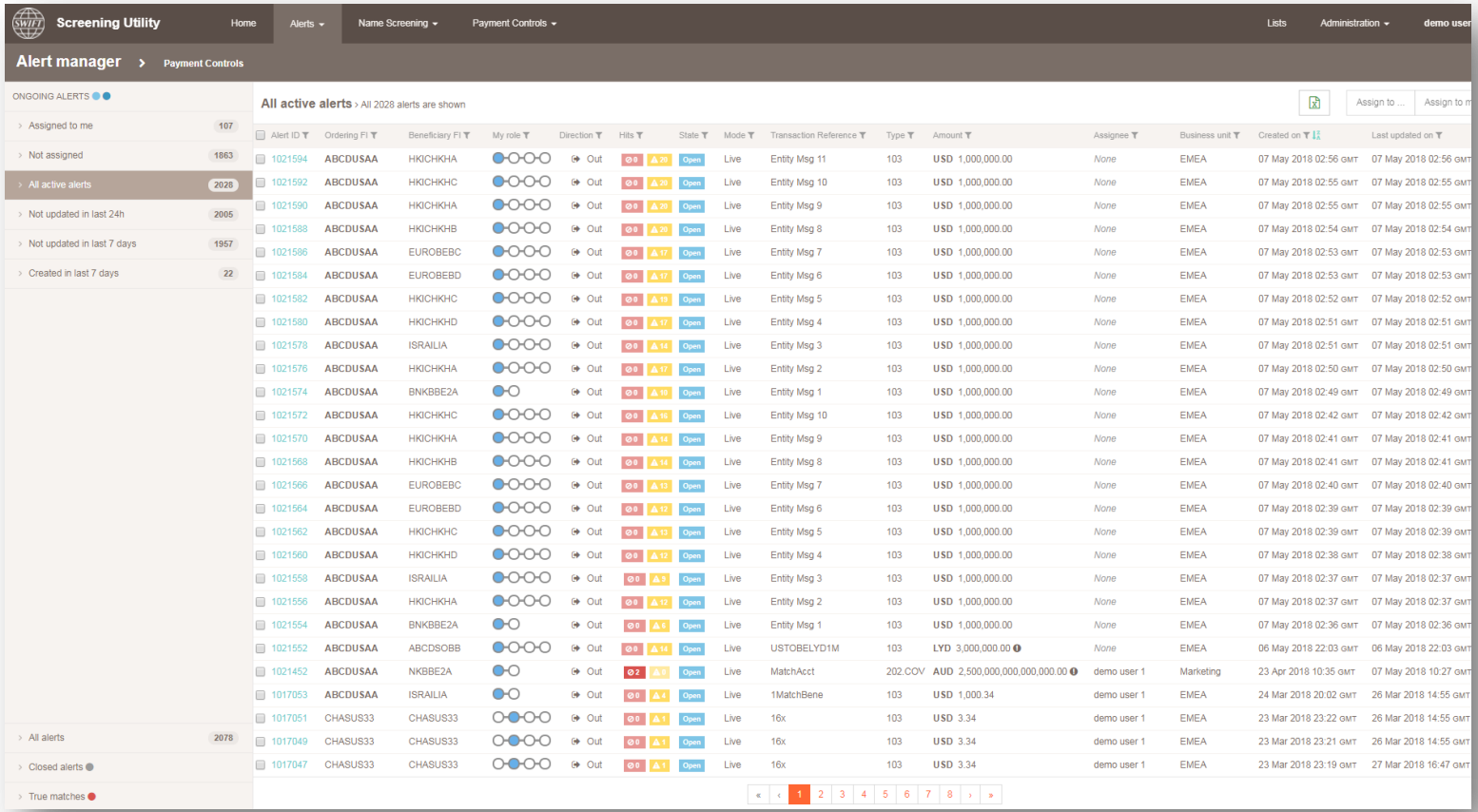
Set up a 'Business calendar' rule

This rule allows you to identify payments made outside of normal working hours or on non-working days.

In this example my institutions normal working hours are Mon-Fri, 8am to 5pm, with the exception of starting at 6am every Friday. I have also created.

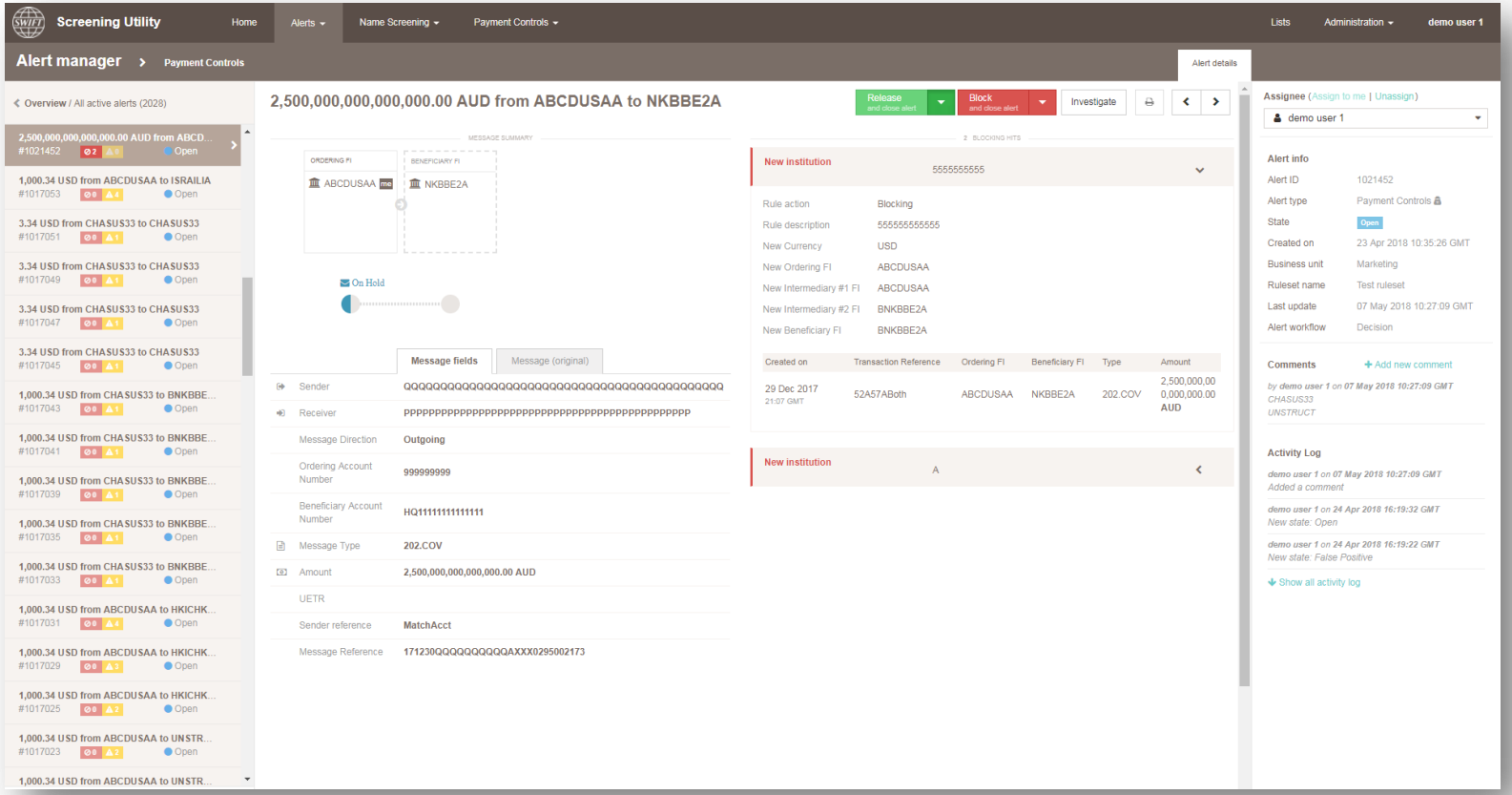
I have also created specific overrides for:

- A working day on the 30th of March, where I am now not sending any payments
- 7th of May which is a bank holiday but I am going to send payments between 8am to 5pm



Alert Manager provides an "inbox" for all Payment Controls alerts that allows you to:

- Easily **identify the key participants** in the transactions – your institution's role and originator and beneficiary
- **Prioritise alerts** based on why they have triggered and operational mode (blocking, non-blocking or test alerts)
- Understand the progression of the alert through the **workflow**
- Capture key **transaction details**



Alert screens provide a complete picture of information:

- Navigate quickly and easily through alerts
- Quickly view the position of the payment within the payment flow
- Easily understand the full content of the payment instruction and the associated rule(s) that triggered the alert
- View related transaction information
- Navigate through the workflow to release held payments or escalate for further review

Preguntas y Respuestas

¡Gracias!

www.swift.com