



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

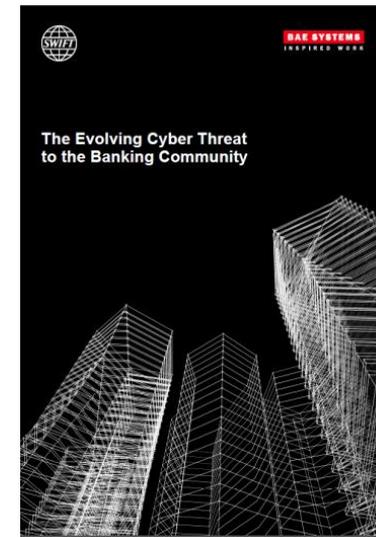
- Attacker impersonate the operator / approver and submits **fraudulent payment instructions**
- May happen outside the normal bank working hours / over public holiday

Step 4

Attackers hide the evidence

Gain time by:

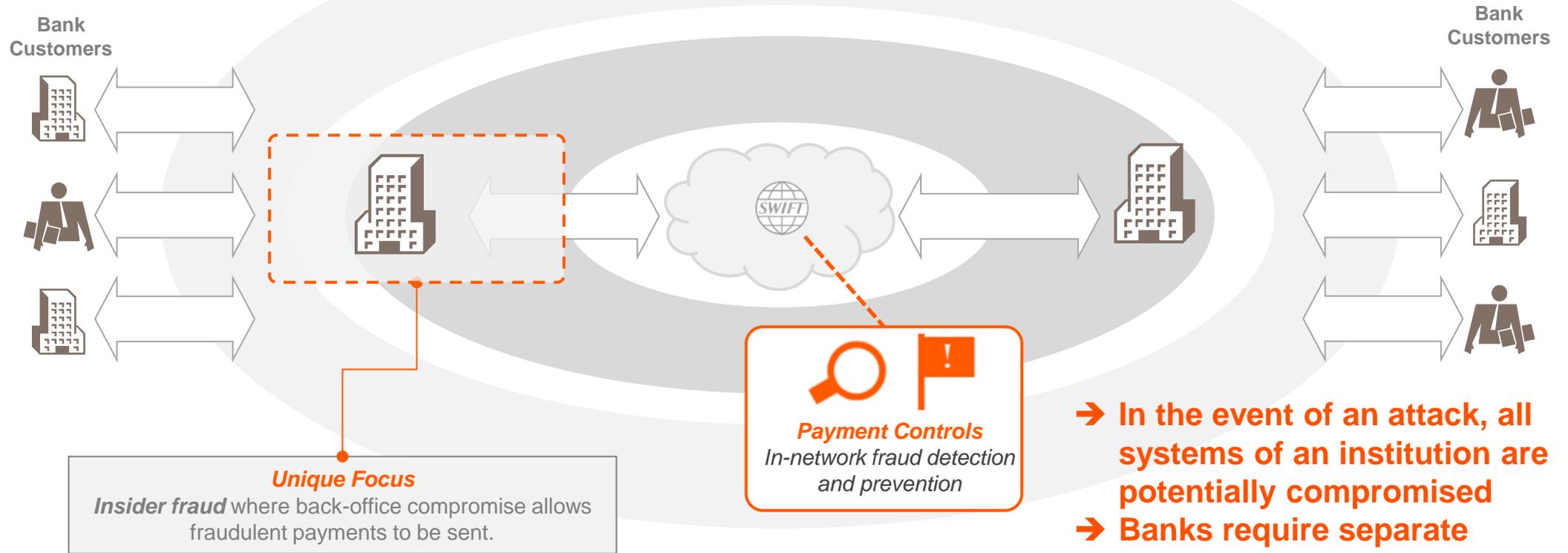
- Deleting or manipulating records / log used in reconciliation
- Wiping Master Boot Record





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” *



Payment Controls | Challenges the industry faces

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 **alerting & 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



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

Daily Validation Reports Documentation & Support
DEMOGBXX 30 Nov 2016

Activity Reports

View aggregate daily activity, maximum value of single transactions and comparison to daily averages

[View your outbound activity >>](#)

Message type	Messages sent	Average amount sent (converted)	USD
MT103	2,009	372,823,991.20	
MT202	1,215	58,647,655,880.27	
MT202C	312	20,515,310.80	

[View your inbound activity >>](#)

Message type	Messages received	Amount received (converted)	USD
MT103	1,834	300,709,597.31	
MT202	530	22,484,895,559.08	
MT202C	134	2,793,031.03	

Risk Reports

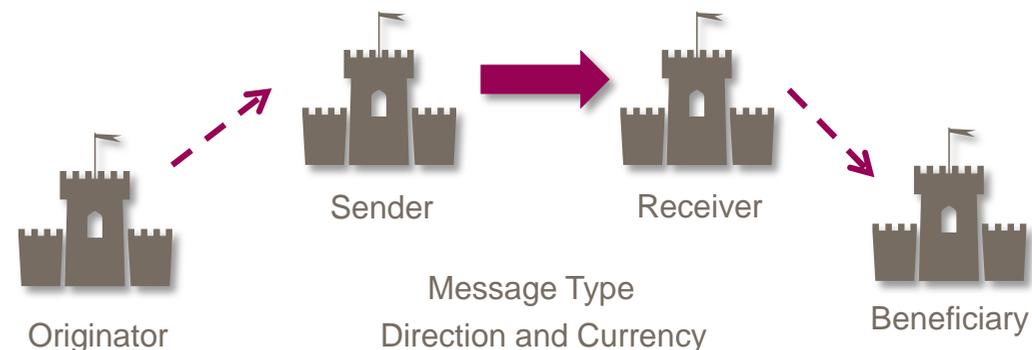
Highlight large or uncharacteristic payments flow and identify new relationship combinations

[View your outbound risk >>](#)

Message type	Currency	Largest transaction sent	58 new relationships
MT103	SGD	739,424,841.75	
MT202	SGD	44,653,129,171.48	
MT202C	DKK	22,924,859.17	

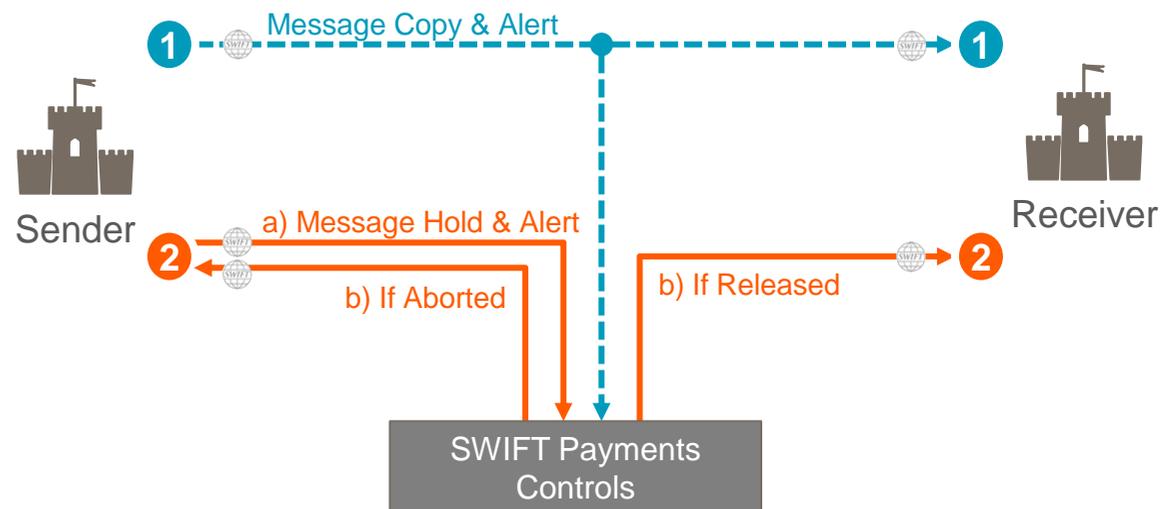
[View your inbound risk >>](#)

Message type	Currency	Largest transaction received	41 new relationships
MT103	SGD	158,142,384.34	
MT202	SGD	22,061,577,176.42	
MT202C	DKK	8,294,917.02	



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**



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

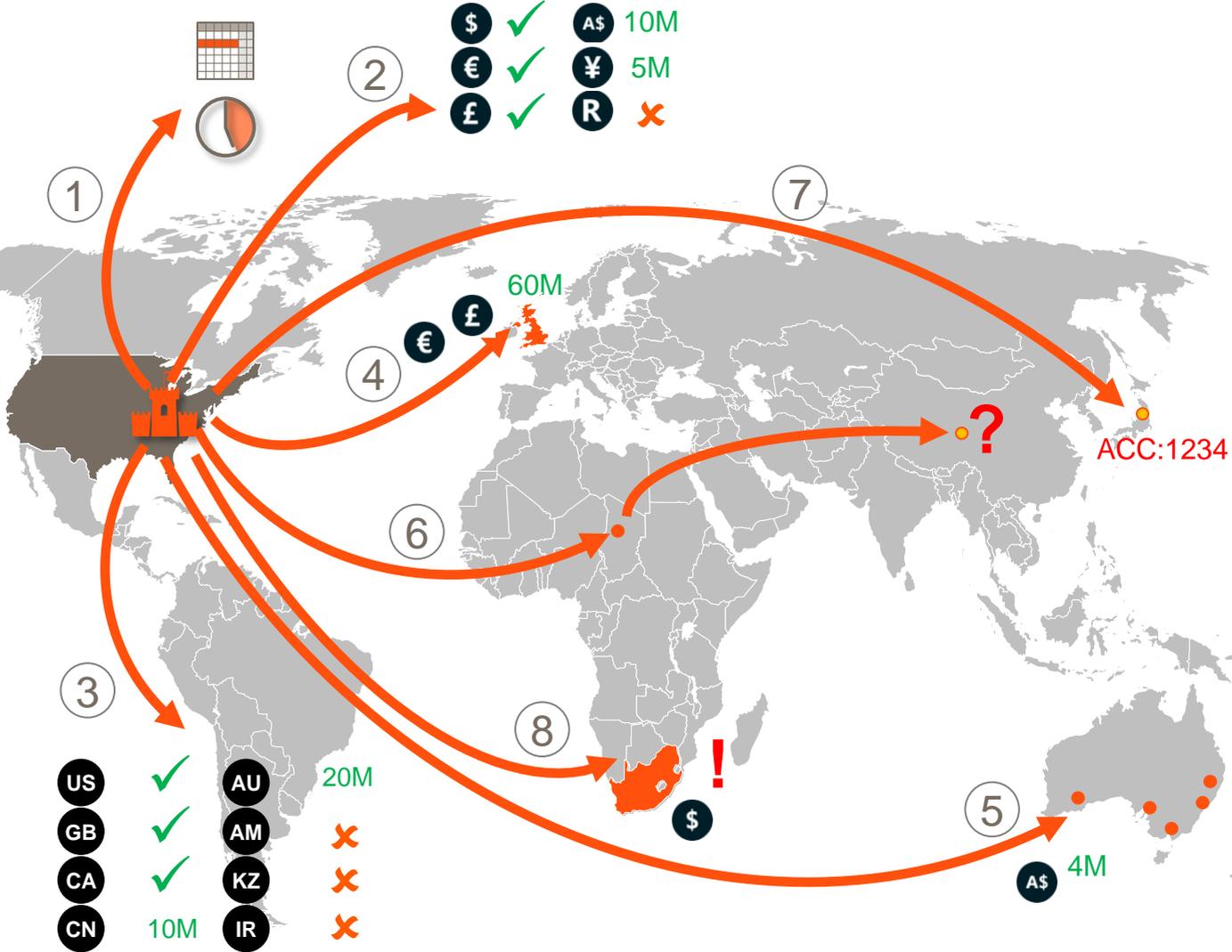
Badly
Formed
Messages

Identify and stop messages where preceded by repetitive NACKs to the same recipient

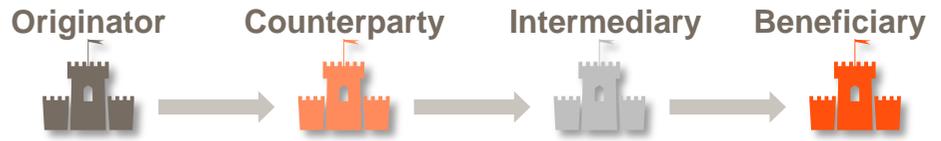
2019

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



Welcome to SWIFT Screening Utility

Configuration (Manage rulesets)

Name Screening service at a glance | Payment Controls service at a glance

Users & BU
Administration
Define business units (Optional) and assign the required roles to users
• User administrator

Policy
Configuration
Define your payment policy and controlling parameters
• Business Administrator
• Ruleset Activator
Refine your payment policy and controlling parameters

Alerts
Alert handling
Handle the alerts that have been generated on your traffic
• L1 Fraud Detection Officer
• L2 Fraud Detection Officer
• Fraud Detection manager

Payment Controls

- Payment Controls service enables you to screen your payment instructions to detect illicit or unusual message flows.
- The screening of your messages is done based on your monitoring policy and controlling parameters. These have to be defined using the Rules Configuration tool.
- Messages that are detected as being illicit or unusual generate alerts which can be accessed and handled via the Alert Management, allowing your organization to investigate the situation.

Rule Configuration

Alerts

Administration

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.

Screening Utility

Home Alerts Name Screening Payment Controls Lists Administration PCS Demo user 1

Configuration

Rulesets

Ruleset	Status	Version	Owning BU	Publication date
FIN PCE DEV	Active Draft	214	EMEA	
Test ruleset	Active Draft	85	Marketing	



Screening Utility Home Alerts Name Screening Payment Controls Lists Administration PCS Demo user 1

Configuration

← Back to overview

Ruleset **Test ruleset** [Edit title and description](#) Previous versions Active Edit draft

Created on	06 Nov 2017 12:09 GMT	Owning BU	Marketing	Current active date	30 Apr 2018 22:26 GMT	Messaging BIC(s)	ABCDUSAA
Last updated on	03 May 2018 15:01 GMT	Last updated by	demo user 1	Current draft date	03 May 2018 15:01 GMT		

Amount aggregation (13) Single payment (31) Message count (47) Mule account monitoring (19) Business calendar (3) New institution (19) Activate Edit alert settings

Live rules (13)

State	Rule action	Ordering	Intermediary #1	Intermediary #2	Beneficiary	Currency	Message Type	Threshold	Rule title	
Edited	Blocking	Me	Any	Any	IN UNSTRUCT, US, GB, FR (COUNTRY)	Any	103, 202 COV	USD 1K	Ablabia	Edit more
	Blocking	Me	IN UNSTRUCT (ENTITY)	Any		Any	103	301 %	GSC - Identify where we send sudden aggregate message value spikes to any individual beneficiary F	Edit more
	Warning	Me	Any	Any	Any	Any	202	USD 100	Me Hee Hee	Edit more
	Warning	Me	Any	Any	IN US, GB, BE, UNSTRUCT (COUNTRY), IN BARC, BONY, CITI (ENTITY)	Any	103	USD 1M	Roy single actor filter - and/or testg	Edit more
	Warning	IN UNSTRUCT (BIC8), IN UNSTRUCT (COUNTRY), IN UNSTRUCT (ENTITY)	Me	Any	Any	Any	103, 202	USD 2	Test amount 28.02	Edit more

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)

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



Edit 'Amount aggregation' rule

1. General information

Rule title *

96/100

Rule description

166/296

Rule action * Decision expiry action *

When the rule is triggered, a blocking hit will be generated that puts the message on hold until the alert is handled

2. Message type selection

Message type *

103 (includes generic MT 103, MT 103 REMIT and MT 103 STP)

202

202.COV

3. Select the actors involved

You must select 'My Institution Role' for one of the Actors

Ordering

Intermediary #1

Intermediary #2

Beneficiary

4. Select which currencies to include

Currency (limit to)

5. Set the aggregation threshold

Aggregation window *

Reference currency

Threshold * % of the normal average with a minimum of US dollars

Specify an absolute value instead

6. Define how the threshold should be counted

- The amount of all transactions is counted together towards a single threshold
- Choose your threshold grouping, based on

Cancel

Save rule

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.



Edit 'New institution' rule

1. General information

Rule title * 32/100

Rule description 41/256

Rule action * 41/256
When the rule is triggered, a non-blocking, acknowledgement-only hit will be generated

2. Message type selection

Message type * 103 (includes generic MT 103, MT 103 REMIT and MT 103 STP)
 202
 202.COV

3. Select the actors involved

You must select 'My Institution Role' for one of the Actors

Ordering

Intermediary #1

Intermediary #2

Beneficiary is in

4. Select which currencies to include

Currency (limit to) is in

Cancel

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.



Edit 'Business calendar' rule

1. General information

Rule title * 21/100

Rule description 47/256

Rule action * Decision expiry action * 47/256

When the rule is triggered, a blocking hit will be generated that puts the message on hold until the alert is handled

2. Message type selection

Message type *

103 (includes generic MT 103, MT 103 REMIT and MT 103 STP)

202

202_COV

3. Define regular working hours

Applicable from * Applicable to *

	Working day start	Working day end	00:00	06:00	12:00	18:00	00:00
Monday	<input type="text" value="08"/> <input type="text" value="00"/>	<input type="text" value="17"/> <input type="text" value="00"/>					
Tuesday	<input type="text" value="08"/> <input type="text" value="00"/>	<input type="text" value="17"/> <input type="text" value="00"/>					
Wednesday	<input type="text" value="08"/> <input type="text" value="00"/>	<input type="text" value="17"/> <input type="text" value="00"/>					
Thursday	<input type="text" value="08"/> <input type="text" value="00"/>	<input type="text" value="17"/> <input type="text" value="00"/>					
Friday	<input type="text" value="06"/> <input type="text" value="00"/>	<input type="text" value="17"/> <input type="text" value="00"/>					
Saturday	<input type="text" value="00"/> <input type="text" value="00"/>	<input type="text" value="00"/> <input type="text" value="00"/>					
Sunday	<input type="text" value="00"/> <input type="text" value="00"/>	<input type="text" value="00"/> <input type="text" value="00"/>					

4. Set optional overrides for specific dates

	Working day start	Working day end	00:00	06:00	12:00	18:00	00:00
<input type="text" value="2018-03-30"/>	<input type="text" value="00"/> <input type="text" value="00"/>	<input type="text" value="00"/> <input type="text" value="00"/>					
<input type="text" value="2018-04-02"/>	<input type="text" value="08"/> <input type="text" value="00"/>	<input type="text" value="17"/> <input type="text" value="00"/>					
<input type="text" value="2018-05-07"/>	<input type="text" value="08"/> <input type="text" value="00"/>	<input type="text" value="17"/> <input type="text" value="00"/>					

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

Screening Utility Home Alerts Name Screening Payment Controls Lists Administration demo user

Alert manager Payment Controls

ONGOING ALERTS ●●

Assigned to me 107

Not assigned 1863

All active alerts 2028

Not updated in last 24h 2005

Not updated in last 7 days 1957

Created in last 7 days 22

All alerts 2078

Closed alerts ●

True matches ●

All active alerts > All 2028 alerts are shown

Alert ID	Ordering FI	Beneficiary FI	My role	Direction	Hits	State	Mode	Transaction Reference	Type	Amount	Assignee	Business unit	Created on	Last updated on	
1021594	ABCDUSAA	HKCHKHA	●○○○○	Out	0	▲ 20	Open	Live	Entity Msg 11	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:56 GMT	07 May 2018 02:56 GMT
1021592	ABCDUSAA	HKCHKHC	●○○○○	Out	0	▲ 20	Open	Live	Entity Msg 10	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:55 GMT	07 May 2018 02:55 GMT
1021590	ABCDUSAA	HKCHKHA	●○○○○	Out	0	▲ 20	Open	Live	Entity Msg 9	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:55 GMT	07 May 2018 02:55 GMT
1021588	ABCDUSAA	HKCHKHB	●○○○○	Out	0	▲ 20	Open	Live	Entity Msg 8	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:54 GMT	07 May 2018 02:54 GMT
1021586	ABCDUSAA	EUROBEBE	●○○○○	Out	0	▲ 17	Open	Live	Entity Msg 7	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:53 GMT	07 May 2018 02:53 GMT
1021584	ABCDUSAA	EUROBEBD	●○○○○	Out	0	▲ 17	Open	Live	Entity Msg 6	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:53 GMT	07 May 2018 02:53 GMT
1021582	ABCDUSAA	HKCHKHC	●○○○○	Out	0	▲ 19	Open	Live	Entity Msg 5	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:52 GMT	07 May 2018 02:52 GMT
1021580	ABCDUSAA	HKCHKHD	●○○○○	Out	0	▲ 17	Open	Live	Entity Msg 4	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:51 GMT	07 May 2018 02:51 GMT
1021578	ABCDUSAA	ISRAILIA	●○○○○	Out	0	▲ 14	Open	Live	Entity Msg 3	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:51 GMT	07 May 2018 02:51 GMT
1021576	ABCDUSAA	HKCHKHA	●○○○○	Out	0	▲ 17	Open	Live	Entity Msg 2	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:50 GMT	07 May 2018 02:50 GMT
1021574	ABCDUSAA	BNKBBE2A	●○○○○	Out	0	▲ 19	Open	Live	Entity Msg 1	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:49 GMT	07 May 2018 02:49 GMT
1021572	ABCDUSAA	HKCHKHC	●○○○○	Out	0	▲ 19	Open	Live	Entity Msg 10	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:42 GMT	07 May 2018 02:42 GMT
1021570	ABCDUSAA	HKCHKHA	●○○○○	Out	0	▲ 14	Open	Live	Entity Msg 9	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:41 GMT	07 May 2018 02:41 GMT
1021568	ABCDUSAA	HKCHKHB	●○○○○	Out	0	▲ 14	Open	Live	Entity Msg 8	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:41 GMT	07 May 2018 02:41 GMT
1021566	ABCDUSAA	EUROBEBE	●○○○○	Out	0	▲ 11	Open	Live	Entity Msg 7	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:40 GMT	07 May 2018 02:40 GMT
1021564	ABCDUSAA	EUROBEBD	●○○○○	Out	0	▲ 12	Open	Live	Entity Msg 6	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:39 GMT	07 May 2018 02:39 GMT
1021562	ABCDUSAA	HKCHKHC	●○○○○	Out	0	▲ 11	Open	Live	Entity Msg 5	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:39 GMT	07 May 2018 02:39 GMT
1021560	ABCDUSAA	HKCHKHD	●○○○○	Out	0	▲ 12	Open	Live	Entity Msg 4	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:38 GMT	07 May 2018 02:38 GMT
1021558	ABCDUSAA	ISRAILIA	●○○○○	Out	0	▲ 5	Open	Live	Entity Msg 3	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:37 GMT	07 May 2018 02:37 GMT
1021556	ABCDUSAA	HKCHKHA	●○○○○	Out	0	▲ 12	Open	Live	Entity Msg 2	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:37 GMT	07 May 2018 02:37 GMT
1021554	ABCDUSAA	BNKBBE2A	●○○○○	Out	0	▲ 6	Open	Live	Entity Msg 1	103	USD 1,000,000.00	None	EMEA	07 May 2018 02:36 GMT	07 May 2018 02:36 GMT
1021552	ABCDUSAA	ABCDSOBB	●○○○○	Out	0	▲ 14	Open	Live	USTOBELOYD1M	103	LYD 3,000,000.00	None	EMEA	06 May 2018 22:03 GMT	06 May 2018 22:03 GMT
1021452	ABCDUSAA	NKBBE2A	●○○○○	Out	0	▲ 0	Open	Live	MatchAcct	202.COV	AUD 2,500,000,000,000,000.00	demo user 1	Marketing	23 Apr 2018 10:35 GMT	07 May 2018 10:27 GMT
1017053	ABCDUSAA	ISRAILIA	●○○○○	Out	0	▲ 4	Open	Live	1MatchBene	103	USD 1,000.34	demo user 1	EMEA	24 Mar 2018 20:02 GMT	26 Mar 2018 14:55 GMT
1017051	CHASUS33	CHASUS33	●○○○○	Out	0	▲ 1	Open	Live	16x	103	USD 3.34	demo user 1	EMEA	23 Mar 2018 23:22 GMT	26 Mar 2018 14:55 GMT
1017049	CHASUS33	CHASUS33	●○○○○	Out	0	▲ 1	Open	Live	16x	103	USD 3.34	demo user 1	EMEA	23 Mar 2018 23:21 GMT	26 Mar 2018 14:55 GMT
1017047	CHASUS33	CHASUS33	●○○○○	Out	0	▲ 1	Open	Live	16x	103	USD 3.34	demo user 1	EMEA	23 Mar 2018 23:19 GMT	27 Mar 2018 16:47 GMT

1 2 3 4 5 6 7 8 >

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**

The screenshot displays the SWIFT Alert Manager interface. The top navigation bar includes 'Screening Utility', 'Home', 'Alerts', 'Name Screening', 'Payment Controls', 'Lists', 'Administration', and 'demo user 1'. The main content area is titled 'Alert manager > Payment Controls' and shows a list of active alerts on the left. The selected alert is for a payment of 2,500,000,000,000.00 AUD from ABCDUSAA to NKBBE2A. The alert details panel on the right shows the rule action as 'Blocking' and provides a table of transaction details.

Alert details:

2,500,000,000,000.00 AUD from ABCDUSAA to NKBBE2A

Release (and close alert) | Block (and close alert) | Investigate

Assignee (Assign to me | Unassign): demo user 1

Alert info:

- Alert ID: 1021452
- Alert type: Payment Controls
- State: Open
- Created on: 23 Apr 2018 10:35:26 GMT
- Business unit: Marketing
- Ruleset name: Test ruleset
- Last update: 07 May 2018 10:27:09 GMT
- Alert workflow: Decision

Comments: + Add new comment

by demo user 1 on 07 May 2018 10:27:09 GMT
CHASUS33
UNSTRUCT

Activity Log:

- demo user 1 on 07 May 2018 10:27:09 GMT
Added a comment
- demo user 1 on 24 Apr 2018 16:19:32 GMT
New state: Open
- demo user 1 on 24 Apr 2018 16:19:22 GMT
New state: False Positive

[Show all activity log](#)

Message Summary:

ORDERING FI: ABCDUSAA | BENEFICIARY FI: NKBBE2A

On Hold

Message fields:

- Sender: QQQ
- Receiver: PPP
- Message Direction: Outgoing
- Ordering Account Number: 999999999
- Beneficiary Account Number: HQ111111111111111
- Message Type: 202.COV
- Amount: 2,500,000,000,000.00 AUD
- UETR
- Sender reference: MatchAcct
- Message Reference: 1712300QQQQQQQQXX0295002173

Transaction Details Table:

Created on	Transaction Reference	Ordering FI	Beneficiary FI	Type	Amount
29 Dec 2017 21:07 GMT	52A57ABoth	ABCDUSAA	NKBBE2A	202.COV	2,500,000.00 0,000,000.00 AUD

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