Sanctions Screening Webinar

Didier BOLLAERTS, Asma BAURTALLY
9, 10 & 11 JULY 2019
Agenda

1. WebAccess migration – *Mandatory Change*

2. New Sanctions lists & New Categories & Message types– *Enhancement*

3. Screening & industry best practices
1- Web Access Migration to simplify access to SWIFT Platforms **Mandatory.**

**Why:** Streamline access to SWIFT services & prepare for S-connect migration

**How you can get ready:** Configure your firewall to allow connection to the new IP addresses (as in the KB below) – starting from **July**

**Migration delivery date:** by end of Q3

**What changes:** the login /authentication process

- New single URL for *Test* Sanctions Screening (*MV-SIPN & Internet access*)
  
  https://sanctionsscreeningtest.browse.swiftnet.sipn.swift.com

- New single URL for *Live* Sanctions Screening (*MV-SIPN & Internet access*)
  
  https://sanctionsscreening.browse.swiftnet.sipn.swift.com

**What does not change:** The portal and all your configuration & settings

**More info:** Please refer to the Knowledge Base [https://www2.swift.com/kb/#/tip/5023282](https://www2.swift.com/kb/#/tip/5023282)
2-1 New Sanctions lists on Sanctions Screening

**Action:** Review this list of **new** and **available** lists to see if any should be added?

- Indian Ministry of Home Affairs (IMHA)
- Thai Anti-Money Laundering Office (TAMLO & TAMLO-UN)
- South Korea - Financial Services Commission (FSC-SK)
- South Korea - Ministry of Strategy and Finance (MSOF)
- South Korea - Ministry of Strategy and Finance (US EO13572) (SKOR)
- UN Other Measures (UNOM)
  - (Relates to asset freeze applying to North Korean vessels & DE-FLAGGED & Prohibited port entry)

For more information please consult the inventory of lists:

Link: [https://www2.swift.com/knowledgecentre/publications/sanc_scrn_inv_list/](https://www2.swift.com/knowledgecentre/publications/sanc_scrn_inv_list/)
A set of new categories have been added:

- **FX and Commodities** (Categories 3 and 6 – all messages type screened by default – both categories included)

- **Securities** (subset of MTs from category 5)
  - *Restricted Securities messages are*: MTs 502, 503, 509, 513, 514, 515, 516, 517, 518, 519, 527, 530, 540, 541, 542, 543, 558, 559, 565, 578, 586, 592, 595, 596, 598, 599

- **Cash Management & Customer status** (subset of MTs from category 9)
  - *Restricted Cash Management & Customer status messages*: MTs 910, 992, 995, 996, 998, 999

- **New Trade message types** SWIFT STANDARD RELEASE *New Trade message types are available within Sanctions Screening*: MT708, MT744, and MT759
How to create a new e-order to screening additional Message Types:

Step 1
Go to the SWIFT.com (www.swift.com) and open the correct change e-order form for Sanctions Screening.

Step 2
Complete the e-order and confirm the new configuration within the change e-order form. Screenshots on the right.

5.01 – 5.04 allows you to select your new configuration

Note: you have to tick the boxes for all categories you want to screen (including the existing ones)
Screening & Industry
Best practices
Very Important Notes on Alert Management Workflow

- **Standard workflow**: L1 users review alerts and decide if they should be released or escalated. If the L1 user suspects a true hit, the payment will be escalated for further investigation by L2.

- **4-eye workflow**: Both the L1’s decision to release and reject MUST be approved by L2 user.

An institution **should never select both workflows** (4-eye workflow & standard workflow). If both workflows are selected **no alerts will be visible for L2 user and the message cannot be actioned.**
Important Notes on the Hit Reduction Rules

1- Vessel Rule for Payments (VPSUCP/VPSUCN).
   - The purpose of this rule is to suppress the hits on Vessel names if found in specific payment messages (below), (FIN Cat 1 and 2 messages)
     - MTs 101, 102, 102 STP, 103, 103 STP, 103 REMIT, 104, 107, 110
     - MTs 202, 202 COV, 205, 205 COV
     - MT 910
   This rule will suppress alerts unless the hits are found in specific fields, namely: field 70 & field 72

2- Vessel Rule for Trades (VTSUCP/ VTSUCN)
   - The purpose of this rule is to suppress the hits on Vessel names if found in specific trade messages. (FIN Cat 4 and 7 messages)
     - MTs 400, 410, and 412
     - MTs 700, 710, 720, 734, and 750
   This rule will suppress alerts unless the hits are found in specific fields, namely: Field 46A, field 77J & field 72
Important Notes on the Hit Reduction Rules

3- Standard Reference Field (SRSUCP/ SRNBCP) (Copy option only)
• The purpose of this rule is to suppress (or to set to non-blocking) the hits that appear in field 20 Sender Reference, or in one of its variants fields: 20C or 20D, for all the FIN messages

4- Related Reference Field (RRSUCP/ RRNBCP) (Copy option only)
• The purpose of this rule is to suppress (or to set to non-blocking) the hits that appear in field 21 Related Reference or in one of its variants fields: 21A, 21B, 21C, 21D, 21E, 21F, 21G, 21N, 21P, 21R for all the FIN messages

For more information, please refer to the Hit Reduction Rules User Guide
Important Notes on the Exception list creation

The creation of an exception list helps to *reduce the volume of false alerts*, so more focus can be allocated on the remaining fewer alerts.

It is recommended to regularly review the results generated by the XML screening report. This reflects the subset of messages for which alert, either in blocking or non-blocking mode, were raised. This can assist in raising new exceptions.

We recommend a regular review of the exception list, to ensure of its continued effectiveness in preventing false positives being raised.

For more information, please refer to the Knowledge Base:
Exception List usage guidelines [https://www2.swift.com/kb/#/tip/5017682](https://www2.swift.com/kb/#/tip/5017682)
## XML screening report

For more information, please refer to the Knowledge Base:
https://www2.swift.com/kb/#/tip/5020966
**Example 1:**

OFAC7890 ID: Jarraya Khalil (a.k.a. “Said”) is matching on all free text tags that contain “SAID”, “for example: customer said”.

This is matching to OFAC entry only.

Exception: SAID will not work!

To create an effective exception on this record, the following needs to be done:

Reference: Common words
Exception: SAID SOMETHING
Eliminate only IDs: OFAC7890
From Sanctions Screening portal

Create new Exception

- Reference: COMMON_WORDS
- Name: SAID SOMETHING
- Search code: OFAC7890

Buttons: Cancel, Reset, Create
Example 2:

<table>
<thead>
<tr>
<th>Type</th>
<th>Unit</th>
<th>Copy Serv.</th>
<th>In/Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>199</td>
<td>SSCRGEB3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Info**
- **Transaction ref**: TEST
- **Related ref**
- **Sender**: ZYFS8E80XXX
- **Receiver**: ZYOD8EB0XXX
- **Amount**: 0.00
- **Created on**: 2010/06/21 14:24:27
- **Value date**: ?

**Origin**
- **MOSF**:
- **Designation**: UN IRAN
- **Type**: 0

**Synonyms**
- **Name**: SAFETY EQUIPMENT PROCUREMENT (SEP)
- **Additional Information**: SAFETY EQUIPMENT PROCUREMENT
- **City/State**
- **Country**
- **Search codes**
- **Passport**
- **National ID**
- **BIC codes**
- **Confidentiality**: 0
- **Comment**: UN
- **Keywords**: UN

**Hyperlinks**
Industry- Best Practices

Annual review to assess the effectiveness of Sanctions Screening Controls, this includes:

• **Institution & customer base jurisdictions**: Are there new regulations to comply? New clients within new countries to deal with? Domestic or international?

• **New products & services offered by institution**: Cross border transactions or trade related products

• **The volume of transactions & distributions channels**

Depending on the risk appetite of the FIs regular monitoring & control need to be put in place.
How to get information on SWIFT
Operational status notifications

1- at least one contact within the institution MUST be registered to SWIFT.COM and subscribed to Sanctions Screening Operational status notifications.

2- Customers MUST maintain their users contact details to ensure continuous access to latest operational notifications.

Notifications can be either by email AND/OR SMS

This will be reflected in the service description and other clients documentations.

How to subscribe:

Link to ACCESS: https://www2.swift.com/idm/myinfo/notifications.faces
Public sanctions lists update notifications

To receive notifications from public sanctions lists, change and check the source of list:

Link: https://www2.swift.com/sanctions_lists

A SWIFT.COM- access is mandatory to access this report
Online Training Modules - SWIFTSmart

There are TWO modules that have been created on SWIFTsmart:

1- **Sanctions Screening introduction**: This includes the following:
   - Workflows & User roles
   - Sanctions Screening Web Interface
   - Sanctions Lists (public and Commercial lists)

   [SWIFT Smart Introduction to Sanctions Screening Module](#)

2- **Compliance policy module**, this covers the following:
   - Message Type Management
   - Sanctions List Management
   - Private List Management

   [SWIFTSmart Compliance policy Module](#)
Topic to cover for next webinar

1- Private list: Creation for: Company, country, individual
2- Reporting: How to use these reports to create exceptions, interpret the data
3- Why not do both!
4- Other topics of your interest

If there are others topics you would like to learn more about or have more questions

• Asma BAURTALLY
  Asma.BAURTALLY@swift.com

• Didier BOLLAERTS
  Didier.BOLLAERTS@swift.com
Additional collateral

- Sanctions Screening Service Documentation Set
- Getting Started
- Inventory of Lists
- Service Description
- User Guide
- Hit Reducing Rules User Guide
- SWIFT Smart Introduction to Sanctions Screening Module
- SWIFTSmart Compliance policy Module
- How to become a SWIFT.COM user: https://www2.swift.com/search/kb/fetchTip.faces?tip=5019388