

ECB Operations Managers Group

Ad-hoc Call on Thursday, 3 March 2022, 09:30-10:30

SUMMARY OF THE DISCUSSION

The ECB OMG held an ad-hoc call to exchange views on operational implications for back offices in light of the recent sanctions towards Russia and tensions in Ukraine, focusing on areas of the impact of market activities, SWIFT ban, and preparedness to activate contingencies.

1. Major tensions or challenges observed in the back-office side of operations

While most of the members reported to have little exposure to the Russian market and the rouble, some members reported to be quite active on the Russian market and thus are significantly impacted by the latest sanctions imposed.

The affected members stated that the current situation is very complicated and that many clients are concerned about rouble settlement. Some institutions have set up task forces with specialists to cover client requests, provide regular updates on sanctions and their interpretation.

Measures implemented so far include: limiting exposure to rouble and the Russian market, stopping new deals, increasing monitoring activities in the fx market. Some banks have blocked their straight-through processing (STP) on fx transactions in rouble and release payments manually, ensuring to receive the counter value before paying. Another aggravating factor is the fact that the rouble is not an eligible currency for CLS. Rouble payments are settling with delay. Some banks are changing their clearing house in order to settle remaining fx transactions. Some banks are distributing deals over smaller amounts to increase likelihood for settlement.

There is a lot of uncertainty regarding the application of sanctions from the EU, UK and US. For example coupon and redemption payments are not impacted by EU sanctions but by US sanctions.

Most members reported an exceptionally high work load on operational and compliance staff to interpret the sanctions, cope with blocked or delayed payments, handle payments manually following the stop of STP and a significant number of calls from customers that are in contact with Russian banks.

2. Operational implications for your back office of the banning of individual institutions from SWIFT

A member acknowledged the fact that it is very difficult to handle the ban of individual Russian institutions from SWIFT.

Another member reported that few market trades are blocked due to the sanctions and that its bank is trying to change the clearing house. FX trades of sanctioned banks that have closed in Europe seem to settle with delay.

3. Preparedness on your side for contingency measures should attacks on SWIFT or payment systems materialise

The vast majority of the members reported that they have robust business continuity measures in place should attacks on SWIFT or payment systems materialise. Cyber security has a very high priority for most banks. Monitoring has been increased, but no reports on increased attempts.

Measures have been stepped up since a while and simulation exercises conducted to test the preparedness in case of a real cyber attack on the bank or access to SWIFT or the payment system. Most members confirmed that a temporary attack on SWIFT affecting an individual organisation could be handled, but a longer shut down of SWIFT would pose a major challenge due to the key market dependence on it.

Some members reported that the manual contingencies would only work for low numbers of high value payments and that they prepared for alternative scenarios routing domestic payments into the domestic payment systems. The use of alternative means seems to be very challenging and not sustainable, in particular for cross-border payments.

Therefore, they suggest that a sectoral approach would be necessary.

4. Other issues reported

A member reported that on a humanitarian side, it seems challenging to provide euro to Ukrainian refugees entering in neighbour countries as the market for Ukraine's local currency UAH against other currencies is not functioning. Banks are looking into solutions to provide support.