Sanctions against Russia: the role of SWIFT

By Mathieu Gex, Marie-Aline Vives

In response to Russia's military invasion of Ukraine, the Council of the European Union has adopted a series of restrictive economic and financial measures, including the exclusion of seven Russian and three Belarusian banks from the SWIFT global financial messaging system. This blog post explains the key role SWIFT plays in the international financial ecosystem.

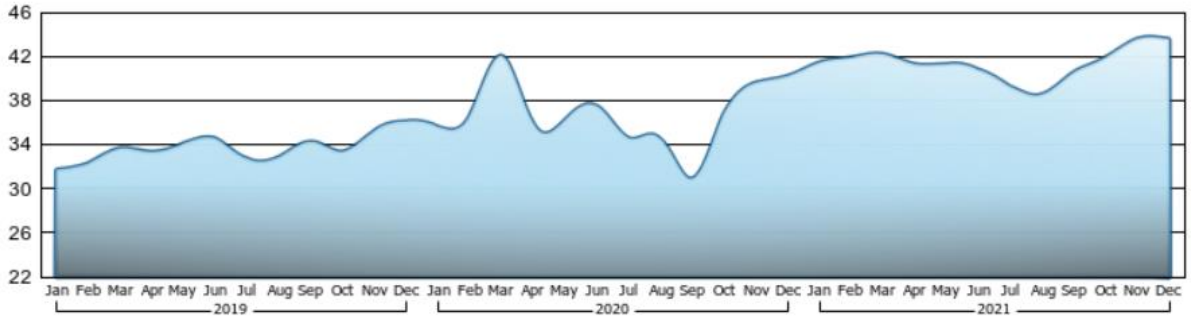

Chart 1. Increase in daily SWIFT traffic over the last three years (in millions of messages)

Source: SWIFT.

SWIFT, a key player at the heart of financial transactions

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a limited liability cooperative company incorporated in Belgium that provides messaging and connectivity services to financial institutions and market infrastructures.

Created in 1973, SWIFT acts as an intermediary between member financial institutions by enabling them to exchange messages containing settlement instructions, notably after carrying out transactions. SWIFT does not perform the actual settlement, but ensures that the relevant instructions are exchanged in the form of standardised messages setting out the terms of the transaction (identification of the securities, price, quantity to be exchanged, date of settlement, counterparties, etc.). A SWIFT confirmation is a binding contract between parties. SWIFT also provides members with access to its messaging network, enabling them to securely transmit information with a guarantee of confidentiality, integrity and non-repudiation (for example, a bank cannot repudiate a message it has sent via the network or, conversely, deny a message it has received).

With over 11,000 users in 200 countries, SWIFT has unrivalled international reach and in 2021 transmitted a total of 10.6 billion messages. SWIFT is therefore deemed to be a "critical service provider" as the extensive use of its services by financial institutions and market infrastructures creates interlinkages that make it of "systemic importance"

The exclusion of SWIFT members: an exceptional measure

SWIFT is owned and controlled by its users and its governance is organised by groups of countries. Its clients are represented on the Board of Directors in proportion to their usage of the messaging services. As a telecommunications service provider, SWIFT is also governed by the principle of neutrality which means it cannot decide to adopt political or economic sanctions against its clients. It can only partially or fully suspend its services for reasons of maintenance, IT security or resilience, to comply with the law or a legal decision, or if a client violates its contractual obligations.

Within this framework, as it is subject to European and Belgium law, SWIFT must comply with the decisions of the Council of the European Union (EU), including those concerning the exclusion of its clients. On this basis, in 2012, it excluded Iranian banks from the network. On 12 March this year, in accordance with the EU Council regulations of 2 and 9 March 2022, SWIFT banned seven Russian banks from the network, after previously informing all stakeholders and the SWIFT community in general, and on 20 March excluded three Belarusian banks. Technically, excluding a bank means removing their Bank Identification Code (BIC) from the register so that they can no longer send or receive messages.

The excluded players could try to use alternative, manual solutions; however these are operationally more cumbersome, and hence slower and less efficient (for example, all linked counterparties have to use the same solutions). If they try to get around the exclusion by using partner banks, then the latter could also be deemed to be in breach of the sanctions.

The sanctioned banks could also try to use alternatives to SWIFT, with the Russian system SFPS or the Chinese system CIPS frequently cited as potential options. However, these systems do not have the same global reach as SWIFT and do not necessarily provide the same functions. Other more unconventional alternatives have also been mentioned, including the use of crypto-assets. However, this solution is unlikely, especially for interbank payments and non-financial corporation transactions.

Reinforced oversight of SWIFT

Due to SWIFT's systemic nature, its smooth operation is vital to the stability of the global financial system. SWIFT is therefore subject to a system of cooperative oversight that was set up in 2004 and comprises the central banks of the G10 countries (Germany, Belgium, Canada, France, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom and the United States), together with the European Central Bank.

The system operates under the aegis of the Banque Nationale de Belgique (BNB) and comprises four main bodies:

- The SWIFT Cooperative Oversight Group (OG) consists of the G10 central banks and the Chairperson of the CPMI (the Bank for International Settlements' Committee on Payments and Market Infrastructures), and decides on the strategy and policy for the oversight of SWIFT.

- The Executive Group (EG), for which the BNB is also lead overseer, consists of the US Federal Reserve Board, the Bank of England, the Bank of Japan and the ECB, and

represents the OG at high-level discussions with SWIFT, passing on its decisions and recommendations.

- The G10 Technical Group (TG) handles technical issues and reports back to the OG.
- The SWIFT Oversight Forum (SOF) is a forum for exchange between the G10 central banks and 15 additional central banks chosen on the basis of their share in total SWIFT traffic volume and on the composition of the CPMI. It communicates information on the SWIFT oversight policy and its priorities, and on the system interdependencies related to the common use of SWIFT.

In the context of the current crisis, oversight of SWIFT has been reinforced. Participants in the oversight framework are closely monitoring the application of the EU sanctions, and are paying particular attention to cyber risk as crises can often lead to an increased risk of cyberattacks.

More broadly, the Banque de France, as a supervisor of financial market infrastructures, is strengthening its oversight in the current crisis. This applies both to its cooperative oversight of European and international infrastructures, and to its direct oversight of the three systemic French market infrastructures – the central counterparty, LCH SA, the central securities depository, Euroclear France, and the retail payments system, CORE(FR). The Banque de France publishes a regular report on its supervision of financial market infrastructures which is available to the public.

The Banque de France is also keeping a close eye on how the market movements observed since the start of the conflict might affect the market infrastructures that it monitors directly. It is also making sure that these infrastructures fully comply with the applicable texts in the current context, and is monitoring their resilience, especially in terms of cybersecurity.