Ukraine and Russia Geopolitical Issues and Sanctions FAQ Updated

ID	Last update	Product & release	Change request	Found in	Fixed in
5025257	02 March 2022	FIN	-	-	-

Ukraine and Russia Geopolitical Issues and Sanctions FAQ

Description

FAQs for Russian financial sanctions

Sanctions affecting connectivity to Russian banks

BICs subject to disconnection

Information

16:00 GMT, 2 March, 2022

- We understand that at this time SWIFT customers may have requests for information. Due to the large number of customers around the world, we are unable to complete individual questionnaires at present.
- Recognising this need, we are keeping the community informed through these continually updated FAQs and via our regular support and customer communications channels.
- We appreciate your understanding and encourage you to check these resources regularly for the latest updates and information.

What is the status of sanctions affecting SWIFT connectivity for Russian banks?

- As a neutral utility with a global systemic character, SWIFT acts in the interests of the entire member community and plays a pivotal role in supporting the global economy through its provision of secure financial messaging services. Any decision to impose sanctions on countries or individual entities rests with the competent government bodies and applicable legislators. SWIFT is and always has been in full compliance with applicable sanctions.
- On 1 March 2022, pursuant to international and multilateral action to intensify financial sanctions against Russia, EU Council Regulation (EU) 2022/345 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine was passed. This regulation prohibits specialised financial messaging providers, such as SWIFT, from providing such services as of 12 March 2022 to entities designated therein. SWIFT is incorporated under Belgian law and must comply with this regulation. Consequently, SWIFT will disconnect access of designated Russian entities to the messaging system on 12 March 2022.

What entities and BICs are impacted?

- The following entities are listed in the EU regulation:
  - Bank Otkritie
  - Novikombank

    - Promsvyazbank
    - Bank Rossiya
    - Sovcombank
    - VNESHECONOMBANK (VEB)
    - VTB BANK

- These are the BICs that will be impacted.

VTBRRUMM	JSC VTB BANK
VTCARUMM	JSC VTB CAPITAL
MOSWRUM2	BM-BANK JOINT-STOCK COMPANY
POSBRUMM	POST BANK JOINT STOCK COMPANY
CNOVRUMM	NOVIKOMBANK JSC
PRMSRUMM	Promsvyazbank PJSC
JSNMRUMM	BANK OTKRITIE FINANCIAL CORPORATION(PUBLIC JOINT-STOCK COMPANY)
OBJSRUMM	OTKRITIE BROKER JOINT STOCK COMPANY
RUIDRUMM	ROSGOSSTRAKH BANK
ROSYRU2P	The Rossiya Bank
SOMRRUMM	SOVCOMBANK
DALVRU8X	ORIENT EXPRESS BANK
BFEARUMM	VEB Bank (Vnesheconombank)
EXIRRUMM	Eximbank of Russia JSC

When will disconnection take place?

- This Regulation requires us to disconnect the identified entities on 12 March 2022, and we will do so accordingly. The SWIFT community will be kept regularly updated across multiple channels.
- We will notify customers when that process starts and as it is implemented via the methods outlined below.

What are the steps for a disconnection?

- In the first instance, a pre-notification will go out to key stakeholders confirming SWIFT's intention to comply with applicable sanctions and initiate the disconnection process.
- Subsequently, the affected entities and related Service Bureau will be notified of the disconnection.
- SWIFT will then initiate the disconnection through our standard provisioning process at the time specified in the notification.
- Once completed, a broadcast will be sent to the community informing them of the disconnection.

How will I know which BICs have been subject to disconnection?

- Once the impacted BICS have been disconnected, a broadcast message will be sent to all FIN users to inform them.
- Deactivated sanctioned BICs are removed from the online directories and will get the updated status "D" (Deleted) in the other directories as of the next monthly update.
- We continuously monitor ongoing developments and if there is any change to the status of sanctioned BICs we will advise by broadcast.

What happens if I have messages in flight at the time of disconnection?

- In line with SWIFT policies, all messages still in queue at the time of disconnection/suspension/deactivation would automatically be aborted, and no subsequent retrieval would be possible. In such cases, the "new" status of deactivated BICs is shown as "obsolete" in the free BIC search on swift.com main page as of the deactivation date.

How do I prevent my back office system sending messages to the deactivated BICs?

- You should both revoke and reject the RMA authorizations with the deactivated BICs. This will prevent your CBT from sending authenticated messages. You can also remove the deactivated BICs from the correspondent file of your CBT to force your CBT to reject messages to these BICs before they are sent to the SWIFT network.

What will happen to a message I send to a deactivated bank?

- The message will be marked with error code H50

What will happen to a file I send over SWIFTNet to a deactivated bank?

- The file will be rejected with a CUG error.

What will happen to a message in which I use the BIC of a deactivated bank in the body of the message text?

- The message will be NAKed with error code T28

How can I identify messages NAKed due to imposed sanctions?

- NAKs will work as usual, they arrive on your SWIFT interface as per normal practice.
- In addition, SWIFT will send you an MT066 Solicited Undelivered Message Report in reply to your MT046 Undelivered Message Report Request. You can specify in your request if you want the MT066 reply to give you all undelivered messages at report time or all undelivered messages for more than nn hours (nn = range between 1 and 24 hours). In the reply MT066 you can find the message status in field 341.

Will the deactivation of these banks be permanent? Will other banks be added and/or removed and if so, where can we find the latest updated list?

- We continuously monitor regulatory developments relevant to SWIFT's operations. As per standard process, we will advise on any further adjustments via a broadcast message.

If the banks are reinstated on SWIFT, what will I have to do to communicate with them again?

- You will have to reintroduce the BICs in the correspondent file of your CBT and you will have to re-initiate any revoked RMA authorization.

Will correspondent banks that have sent messages to these banks in the past be able to put in a request to SWIFT to retrieve these messages?

- Correspondent banks (sending or receiving customers) can put in a request to SWIFT to retrieve message data in accordance with the SWIFT Data Retrieval Policy. As per this policy, they can either: i) request retrieval when this possibility is offered as part of the SWIFT services and products, as is documented in the relevant service description; or ii) request mass retrievals of their message data in an emergency or other exceptional circumstance.
- For the sake of clarity, upon deactivation, deactivated customers can no longer request nor authorise retrieval of their messages.

In the event a bank is disconnected from the network, what is the impact on their contracts for the various products and services provided by SWIFT?

- If a bank is disconnected from the SWIFT network, all its underlying contracts are terminated.

In the event a bank is subjected to US technology-related sanctions, what is the impact on SWIFT products and services, such as tokens?

- A bank designated SDN (by US OFAC) will not trigger blocking export /re-export of US technology. However, if the bank is designated under US Export control restrictions, then any new shipment of tokens would be blocked. They would still be allowed to use tokens previously acquired.

What cyber security measures does SWIFT currently have in place?

- All SWIFT services are operating as normal.
- SWIFT takes security very seriously and we have a strong control environment in place for physical and cyber security.
- Building on the strong physical and cyber security control environment already in place as part of the baseline threat level at SWIFT, we continuously monitor the threat landscape, which may result in increasing or decreasing our physical and/or cyber threat level.
- Raising the threat level results in additional prevention/detection/response and/or recovery measures. These would typically include increased resourcing focused on intelligence gathering, network scanning, dedicated threat hunting and monitoring for known Indicators of Compromise (IoC) and Tactics, Techniques and Procedures (TTP).
- SWIFT also has relationships with key industry cyber security organizations, including the Financial Services Information Sharing and Analysis Center (FS-ISAC).

What business continuity measures does SWIFT have in place?

- All SWIFT services are operating as normal.
- As part of our normal business continuity preparedness, SWIFT has robust plans in place for all our critical services with the ability to continue normal operations in a crisis situation. We remain ready to activate these plans if necessary.

Can SWIFT help me to comply with sanctions?

- Yes, SWIFT has a wide range of services to help customers meet their responsibilities to comply with national and international legislation, while supporting the resilience and integrity of the global financial system as a global and neutral service provider.
- We offer a range of screening solutions that can be implemented quickly, according to our customers' own risk appetites. The Transaction Screening Service is used by approximately 1,000 institutions to screen SWIFT traffic against the latest sanctions lists, whilst our Payment Controls solution screens transactions as they go over the SWIFT network to help institutions identify anomalies in their traffic, which might indicate a cyber risk or fraud.
- You can find out more about these services here.
- There are also a host of resources available on the SWIFT Knowledge Centre to support you with your sanctions screening requirements, including links to Publications, Knowledge Based Articles, How To Videos, SWIFTSmart courses, and other related products (e.g. Name Screening, Sanctions List Distribution, Transaction Screening).

How quickly will SWIFT be updating in sanctions lists within the Transaction Screening Service (TSS) and Sanctions Screening Service (SSS) products?

- Details (content and timing) of the sanctions list updates are made available to customers on swift.com (SSS) or in the application itself (TSS).

- We attempt to update and activate new lists in a diligent manner, to ensure they are taken into account soon after publication by the regulators or, for commercial third-party lists, soon after being made available by the supplier.
- If we are not able to activate changes to a public sanctions list within a reasonable period upon their publication by the regulator, then we will inform customers about the exact date of activation of such changes in the service.

I am a SWIFT service bureau – where do I direct my customers if they have questions?

- Please send them the link to these FAQs in the first instance.
- For any other questions, please direct them to SWIFT Customer Support.

A scheduled update to one of my SWIFT services didn't happen as planned, when will it happen now?

- Following the sanctions announcement on March 1st by the European Commission, we have had to reprioritise certain releases, updates and installations. We will communicate the new dates as soon as is practically possible via our usual communication channels.

How / where can I view my SWIFT message traffic flows to help me understand the potential impact of the sanctions on my operations?

- If you are a user of our Compliance Analytics tool you can use it to analyse your institution's SWIFT payments traffic and get a view of your branch and correspondent activity.
- You can also use our Traffic Analytics tool within Watch Traffic to analyse your organisation's FIN, INterAct and FileAct traffic volumes.
- For more information, click on the product names above, visit the SWIFT Knowledge Centre or speak to your relationship manager.

Where do I go for further information?

- This page contains the most up to date information and is regularly updated.
- If you have any further questions, please get in touch with your designated SWIFT relationship manager.