Information Paper

SWIFT and the Fight Against Illicit Financial Activity

The challenge facing the financial industry as a whole, in preventing illicit activity, is to implement measures that prevent illegal behaviour without penalising the efficient processing of legitimate financial transactions. SWIFT is fully committed to doing its part to address this challenge.

It is SWIFT policy that our services must not be used to facilitate illegal activities. At the same time, SWIFT is global, thus SWIFT users around the world are not subject to a single set of rules, but to a variety of different compliance rules – such as those that might relate to illicit and terrorist financing.

SWIFT itself does not monitor or control the messages that users send through its system and recognises that all decisions on the legitimacy of financial transactions under applicable regulations rest with the financial institutions handling them, and with their competent international and national authorities. SWIFT users' access to the SWIFT messaging service depends on authorisation from their competent authorities, which can be of course rescinded in the case of non-compliance with such rules.

Our Messaging Services in the cross border context

SWIFT provides messaging services to institutions around the world, effectively acting as a secure postman between its users.

When a bank customer in one country wishes to transfer funds to another bank's customer in another country, the two banks will exchange instructions, confirmations and reports between themselves. Banks exchange this information either using communication mechanisms such as VPN lines, email, telex or fax, or specialised financial messaging providers, such as SWIFT. If the two banks don't have direct relations between themselves, intermediary or correspondent banks will sit between them, so there can be four (or even more) banks involved in a single transfer. As a result, any given transfer relies on the banks concerned exchanging a significant amount of instructions, reports and confirmations on one or more communication channels.

When SWIFT is used as the communication channel, SWIFT simply acts as a virtual messenger, safely transporting the messages – no funds are actually transferred over SWIFT, nor does SWIFT at any point have custody or ownership of funds. SWIFT has no relationship with the ultimate customers that are making the underlying payment through the banking system nor, where intermediaries or correspondents are involved, would SWIFT necessarily always have relationships with the banks' respondents.

Necessarily, KYC, AML and CTF responsibilities both for the payer and the payee sit with the banks that hold the relations with those customers. Additionally, it is increasingly incumbent on those banks acting as intermediaries or correspondents in the process, to ensure that any processing they do for their respondent banks meets their own compliance obligations; in other words – any given transfer needs to be checked for compliance purposes not once, but multiple times, by all the banks involved in processing the transfer, and not against one set of rules, but against multiple sets of rules. Serial checks need to be made throughout the process to ensure that each entity is compliant with the rules and regulations applicable to it and, for instance, that the customers and the

banks involved are screened against the lists of prohibited entities and persons applicable to each bank involved in the chain.

SWIFT provides a growing range of products and services to facilitate its users' compliance with those rules. We also regularly remind our users that SWIFT messaging services should not be used for illegal purposes and that users' access to the SWIFT messaging service depends on authorisation from their competent authorities, which can be of course rescinded in the case of non-compliance with such rules.

Our Focus

As far as illicit finance, AML and CTF compliance are concerned, SWIFT's key focus is threefold – firstly on ensuring our own compliance with applicable rules, secondly on assisting our users in meeting their responsibilities to comply with national and international regulations – whether through the development of appropriate messaging standards, products, processes or services. And, thirdly, SWIFT is fully committed to its policy of cooperation with competent authorities to fight illegal activities within the scope of its activity.

In 2006-2007 we introduced changes to our payment message formats to allow financial institutions to comply with FATF SRVII (Special Recommendation VII on fighting terrorist financing - currently replaced by recommendation 16 of the revised FATF Recommendations 2012) by including more detailed information on the payment ordering customer. In 2010, we also introduced changes to our cover payment messages to allow financial institutions to include underlying customer information of cover payment transactions.

More recently, SWIFT has been closely following the Wire Transfer Regulation (EU regulation 2015/847). In cooperation with our community, we have made the necessary changes to the related message standards. In the MT 103, MT 202.COV and MT 205.COV messages, for instance, we now have two fields (50a and 59a) in which users can embed the required information for ordering and beneficiary customers.

SWIFT is continuing to work with the community on a standards roadmap to ensure the use of structured information and greater transparency in specified message fields by 2020.

Additionally, since the end of 2014 SWIFT has been exploring the potential for a solution to provide insights into the level of data quality within relevant SWIFT messages (MT103, MT202.COV, MT205.COV) relating to FATF Recommendation 16. We have engaged with our users to help understand existing market practice and to test initial software designs. Following the successful conclusion of a proof of concept, SWIFT has since been developing the product which is scheduled to be launched by end of the second quarter of 2016.

SWIFT has a wide and growing range of financial crime compliance tools, including a Know Your Customer facility, the KYC Registry, sanctions screening, testing and a growing range of compliance analytics tools.

We also periodically remind our users of their compliance obligations and we consult with appropriate authorities. In areas or times of heightened risk we take extra precautions in cooperation with appropriate authorities.

Our Cooperation

SWIFT is in full compliance with applicable sanctions and CTF legislation and has a history of cooperating in good faith with authorities such as central banks, treasury departments, law enforcement agencies, as well as with relevant international organisations, such as the Financial Action Task Force (FATF), in their efforts to combat abuse of the financial system for illegal activities.

SWIFT also cooperates with the authorities on terrorism related issues through the Terrorist Finance Tracking Program (TFTP). Shortly after the September 11 attacks, the U.S. Treasury Department (UST) initiated the TFTP, under which UST issues administrative subpoenas for terrorist-related data to SWIFT's US operating centre.

SWIFT's EU Operating Centre complies with what is in effect the same programme, under what is known as the TFTP Agreement. This EU-US Agreement came into effect in August 2010, and is generic in nature in that it applies to any designated provider of messaging services with operations in Europe and in the United States. SWIFT is currently designated under the Agreement and accordingly is subject to legally binding requests to transfer data which is located in its EU Operating Center to the US Treasury for counter terrorism investigation purposes.

The subpoenas in both cases require SWIFT to provide the US Treasury with certain SWIFT messages which are – and can only be – used for counterterrorism purposes. This programme has provided valuable leads to authorities around the world, and more information on the programme can be found here.

Due to the confidential nature of our contacts with authorities and due to non-disclosure and other legal requirements, SWIFT does not comment on them.

Legal notices

About SWIFT
SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services.

We provide our community with a platform for messaging, standards for communicating and we offer products and services to facilitate access and integration; identification, analysis and financial crime compliance.

Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories, enabling them to communicate securely and exchange standardised financial messages in a reliable way.

As their trusted provider, we facilitate global and local financial flows, support trade and commerce all around the world; we relentlessly pursue operational excellence and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies.

Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.

Disclaimer
SWIFT supplies this publication for information purposes only. The information in this publication may change from time to time. You must always refer to the latest available version.

57183 - MAR 2016