Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

FINMA Guidance 02/2019

Payments on the blockchain

26 August 2019

Laupenstrasse 27
3003 Bern
Tel. +41 (0)31 327 91 00
Fax +41 (0)31 327 91 01
www.finma.ch

Introduction

Date:
26 August 2019

In this guidance, FINMA provides information about the application of regulatory requirements for payments on the blockchain for financial services providers under FINMA supervision.

Cryptocurrencies and related technologies create new opportunities for criminals and terrorists to launder their proceeds or finance their illicit activities.[1] In light of this, the Financial Action Task Force (FATF) set about strengthening its standards on virtual assets and completed this work on 21 June 2019. The published guidance on virtual asset service providers (VASPs) deals with blockchain service providers such as exchanges, wallet providers and trading platforms. It requires that the existing rules on combating money laundering also apply to such service providers.

FINMA reaffirms its technology-neutral approach

FINMA recognises the innovative potential of new technologies for the financial markets. It applies the relevant provisions of financial market law regardless of the underlying technology. However, blockchain-based business models cannot be allowed to circumvent the existing regulatory framework. This applies particularly to the rules for combating money laundering and terrorist financing, where the inherent anonymity of the blockchain presents increased risks. For this reason, Switzerland has always applied the Anti-Money Laundering Act to blockchain service providers.[2] Such providers are obliged, for example, to verify the identity of their customers, to establish the identity of the beneficial owner, to take a risk-based approach to monitoring business relationships and to file a report with the Money Laundering Reporting Office Switzerland (MROS) if there are reasonable grounds to suspect money laundering.

Required information in payment transactions

Article 10 AMLO-FINMA requires that information about the client and the beneficiary be transmitted with payment orders. The financial intermediary receiving this information then has the opportunity to check the name of the sender against sanction lists, for example. It can also check whether the

[1] See also the CGMF's report, National Risk Assessment: Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding, October 2018

[2] See also the Federal Council report – Legal framework for distributed ledger technology and blockchain in Switzerland, December 2018

information for the beneficiary is correct or whether it should return the payment in the event of discrepancies.

The provision must be interpreted in a technology-neutral way and therefore also applies to services based on blockchain technology. It is not necessary for the information to be transmitted on the blockchain. Transmission can take place via other communication channels. The purpose of the provision, namely to make it more difficult for sanctioned persons or states to act anonymously in the payment transaction system, is particularly relevant to the blockchain. The FATF also expects information about the client and the beneficiary to be transmitted with token transfers in the same way as for bank transfers.

No system currently exists at either a national or an international level (such as, for example, SWIFT for interbank transfers) for reliably transferring identification data for payment transactions on the blockchain. Neither are bilateral agreements between individual service providers in existence to date. For such systems or such agreements to meet the requirements of Article 10 AMLO-FINMA in future, they would have to involve only service providers who are subject to appropriate anti-money laundering supervision. Unlike the FATF standards, Article 10 AMLO-FINMA does not provide for any exception for payments involving unregulated wallet providers. Such an exception would favour unsupervised service providers and would result in supervised providers not being able to prevent problematic payments from being executed.

As long as an institution supervised by FINMA is not able to send and receive the information required in payment transactions, such transactions are only permitted from and to external wallets if these belong to one of the institution's own customers. Their ownership of the external wallet must be proven using suitable technical means. Transactions between customers of the same institution are permissible. A transfer from or to an external wallet belonging to a third party is only possible if, as for a client relationship, the supervised institution has first verified the identity of the third party, established the identity of the beneficial owner and proven the third party's ownership of the external wallet using suitable technical means.

If the customer is conducting an exchange (fiat-to-virtual currency, virtual-to-fiat currency, or virtual-to-virtual currency) and an external wallet is involved in the transaction, the customer's ownership of the external wallet must also be proven using suitable technical means. If such proof is not available, the above rules for payment transactions apply.