SWIFT's response to the Financial Industry Regulatory Authority on the report: "Distributed Ledger Technology: Implications of Blockchain for the Securities Industry"

[Subject]

SWIFT

31 March 2017

Confidentiality: Public

SWIFT thanks FINRA for the opportunity to provide comments on the report Distributed Ledger Technology: Implications of Blockchain for the Securities Industry.

SWIFT is a member-owned, cooperative society headquartered in Belgium. SWIFT is organised under Belgian law and is owned and controlled by its shareholding Users, comprising over 3,000 financial institutions. We connect more than 11,000 connected firms, in more than 200 countries and territories. A fundamental tenet of SWIFT's governance is to continually reduce costs and eliminate risks and frictions from industry processes.

SWIFT provides banking, securities, and other regulated financial organisations, as well as corporates, with a comprehensive suite of messaging products and services. We support a range of financial functions, including payments, securities settlement, reporting, and treasury operations. SWIFT also has a proven track record of bringing the financial community together to work collaboratively, to shape market practice, define formal standards and debate issues of mutual interest.

If you wish to discuss any aspect of our response please do not hesitate to let us know.

Natasha de Terán

SWIFT | Head of Corporate Affairs

Tel: + 44 20 7762 2151

Mob: + 44 7780 483 467

www.swift.com

Regulatory Considerations: Customer Data Privacy

FINRA clearly states that the protection of financial and personal customer information is a key responsibility and the obligation of all FINRA member firms. As required by Regulation S-P, broker-dealers must have written policies and procedures in place to address the protection of customer information and records. These rules also require firms to provide initial and annual privacy notices to customers describing information sharing policies and informing customers of their rights. As a result broker-dealers would need to consider and account for the application of such customer data privacy requirements to the information maintained or shared on any distributed ledger technology (DLT) network. When joining a DLT network, firms would need to assess whether the network and its policies and procedures are designed appropriately, such that participating firms can meet their obligations associated with customer data privacy.

In a DLT network, however, data (including certain customer information and transaction records) may be shared with all parties on the network. Even when such data is encrypted, it can still be vulnerable to being exposed or accessed by unauthorised parties on the network to whom it has been distributed. Individuals or institutions with malicious intent could use brute force to decrypt the encrypted data; indeed it should be borne in mind that an encryption method that is considered secure at any given point in time can become vulnerable and/or breakable within a five-year period. Thus, depending on the use case and the reputational damage caused by exposing five-year old data, the use of encryption in distributed data has to be approached cautiously.

In the past few months, several implementations have started to address these ledger confidentiality issues. New permissioned ledger technologies (like Quorum and Hyperledger Fabric v1.0) now propose 'selective distribution'. These technologies still involve all participants in the ledger in guaranteeing the integrity of the ledger, but only distribute specific subsets of the data to particular parties as needed. This allows 'smart contract' developers to decide who needs to be involved in each transaction, and access which data. Using this method, it is possible for a set of different smart contracts to coexist on the same ledger, each of them exposing and distributing specific sets of data to specific participants.

SWIFT believes such solutions should be considered to address the regulator's data privacy concerns and members' obligations.

Implementation Considerations: Data and transparency requirements

FINRA correctly states that an important consideration for market participants in implementing a DLT network is determining the operational structure of the network. The operational structure of a DLT network would typically include developing a framework for: (1) network participant access and related on-boarding and off-boarding procedures; (2) transaction validation; (3) asset representation; and (4) data and transparency requirements.

SWIFT believes the additional privacy safeguards achieved through selective distribution that we describe above do not reduce transparency. This same technology can ensure that a regulator is part of any transaction and has visibility on each transaction data, whilst still guaranteeing full privacy vis-à-vis other participants on the ledger who are not part of a particular transaction.

---------- END ----------