GLI GLOBAL LEGAL INSIGHTS

Blockchain & Cryptocurrency Regulation

2021

Third Edition

Contributing Editor: **Josias N. Dewey**

glg global legal group

BLOCKCHAIN ALLIANCE · ENTERPRISE ETHEREUM ALLIANCE · LSTA CELEBRATING 25 YEARS · WSBA WALL STREET BLOCKCHAIN ALLIANCE

Global Legal Insights
Blockchain & Cryptocurrency Regulation

2021, Third Edition
Contributing Editor: Josias N. Dewey
Published by Global Legal Group

GLOBAL LEGAL INSIGHTS – BLOCKCHAIN & CRYPTOCURRENCY REGULATION

2021, THIRD EDITION

Contributing Editor
Josias N. Dewey, Holland & Knight LLP

Head of Production
Suzie Levy

Senior Editor
Sam Friend

Sub Editor
Megan Hylton

Consulting Group Publisher
Rory Smith

Chief Media Officer
Fraser Allan

We are extremely grateful for all contributions to this edition.
Special thanks are reserved for Josias N. Dewey of Holland & Knight LLP for all of his assistance.

Published by Global Legal Group Ltd.
59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 207 367 0720 / URL: www.glgroup.co.uk

ISBN 978-1-83918-077-4
ISSN 2631-2999

Printed and bound by TJ International, Trecerus Industrial Estate, Padstow, Cornwall, PL28 8RW
October 2020

CONTENTS

Country chapters

PREFACE

Another year has passed and virtual currency and other blockchain-based digital assets continue to attract the attention of policymakers across the globe. A lack of consistency in how policymakers are addressing concerns raised by the technology is a major challenge for legal professionals who practice in this area. Perhaps equally challenging is keeping up with the nearly infinite number of blockchain use cases. In 2017 and 2018, it was the ICO craze. In 2019, the focus shifted to security tokens. In 2020, decentralized finance (or DeFi) attracted over several billion dollars' worth of investment. So, while ICOs are still being offered and several groups continue to pursue serious security token projects, we should expect DeFi to draw scrutiny from regulators, such as the U.S. Securities and Exchange Commission (SEC). Once again, legal practitioners will be left to counsel clients on novel issues of law raised by the application of laws and regulations enacted long before blockchain technology existed.

Of course, capital raising is only one application of the technology. Bitcoin, which remains the king of all cryptocurrencies, was intended to serve as a form of digital money. Arguably, it is this use case that has seen the most attention from governments around the word. The European Union enacted more stringent anti-money laundering (AML) regulations impacting virtual currency exchanges operating in the EU. U.S. regulators and state government officials continue to enforce money transmitter statutes and BSA regulations applicable to money services businesses. In the U.S., the state of New York, which was once thought to have over-regulated the industry out of doing business in the state, is now attracting applications from blockchain companies to become state-chartered trust companies. The charter may provide relief to virtual currency exchanges and similar businesses seeking to avoid the nearly 50-state patchwork of licensing statutes.

Institutional and large enterprise companies continue to expand into the space. It is no longer just FinTechs and entrepreneurial clients who need counsel on blockchain-related matters. Whether a small start-up or Fortune 100 company, clients need counsel in areas beyond compliance with government regulation. In some cases, intellectual property rights must be secured, or open source licenses considered to the extent a client's product incorporates open source code. Blockchain technology adopted by enterprise clients may involve a consortium of prospective network users, which raises joint development issues and governance questions.

As with the first two editions, our hope is that this publication will provide the reader with an overview of the most important issues across many different use cases and how those issues are impacted by laws and regulations in several dozen jurisdictions around the globe. And while policymakers continue to balance their desire to foster innovation, while protecting the public interest, readers of this publication will understand the current state of affairs, whether in the U.S., the EU, or elsewhere in the world. Readers may even discover themes across this book's chapters that provide clues about what we can expect to be the hot topics of tomorrow and beyond.

Josias N. Dewey
Holland & Knight LLP

FOREWORD

Dear Industry Colleagues,

On behalf of the Enterprise Ethereum Alliance ("EEA"), I would like to thank Global Legal Group ("GLG") for bringing to life an explication of the state of regulation in the blockchain and cryptocurrency sector, with its third edition publication of *Blockchain & Cryptocurrency Regulation*. GLG has assembled a remarkable group of leaders in the legal industry to analyse and explain the environment in front of us, and the EEA members and participants were pleased to contribute to the publication.

We stand at the beginning of an industry, and the depth and breadth of the contributors from leading law firms across the world only serve to highlight the growing interest and fascination with accelerating the adoption of blockchain technology. We thank each of the authors for taking the time to compose their chapters and for the expertise they demonstrate. We hope readers will find this publication useful.

The EEA is the industry's first member-driven global standards organisation whose mission is to develop open, blockchain specifications that drive harmonisation and interoperability for businesses and consumers worldwide. The EEA's world-class Enterprise Ethereum Client Specification, Off-Chain Trusted Compute Specification, and forthcoming testing and certification programs, along with its work with the Token Taxonomy Initiative, will ensure interoperability, multiple vendors of choice, and lower costs for its members – hundreds of the world's largest enterprises and most innovative startups. For additional information about joining the EEA or the Token Taxonomy Initiative, please reach out to membership@entethalliance.org and info@tokentaxonomy.org.

Sincerely,

Aaron Wright

Chairman, EEA Legal Advisory Working Group

GLOSSARY

***Alice* decision**: a 2014 United States Supreme Court decision about patentable subject matter.

Cold storage: refers to the storage of private keys on an un-networked device or on paper in a secure location.

Copyleft licence: the practice of offering people the right to freely distribute copies and modified versions of a work with the stipulation that the same rights be preserved in derivative works down the line.

Cryptocurrencies: a term used interchangeably with virtual currency, and generally intended to include the following virtual currencies (and others similar to these):

- Bitcoin.
- Bitcoin Cash.
- DASH.
- Dogecoin.
- Ether.
- Ethereum Classic.
- Litecoin.
- Monero.
- NEO.
- Ripple's XRP.
- Zcash.

Cryptography: the practice and study of techniques for secure communication in the presence of third parties, generally involving encryption and cyphers.

DAO Report: report issued in July, 2017 by the U.S. Securities and Exchange Commission, considering and ultimately concluding that The DAO (*see below*) was a security.

Decentralised autonomous organisation ("The DAO"): a failed investor-directed venture capital fund with no conventional management structure or board of directors that was launched with a defect in its code that permitted someone to withdraw a substantial amount of the $130,000,000 in Ether it raised.

Decentralised autonomous organisation ("a DAO"): a form of business organisation relying on a smart contract (*see below*) *in lieu* of a conventional management structure or board of directors.

Digital assets: anything that exists in a binary format and comes with the right to use, and more typically consisting of a data structure intended to describe attributes and rights associated with some entitlement.

Digital collectibles: digital assets that are collected by hobbyists and others for entertainment, and which are often not fungible (e.g., CryptoKitties) (*see* **Tokens**, non-fungible).

Digital currency: a type of currency available only in digital form, which can be fiat currency or virtual currency that acts as a substitute for fiat currency.

Digital currency exchange: a business that allows customers to trade cryptocurrencies or digital currencies for other assets, such as conventional fiat money, or one type of cryptocurrency for another type of cryptocurrency.

Digital/electronic wallet: an electronic device or software that allows an individual to securely store private keys and broadcast transactions across a peer-to-peer network, which can be hosted (e.g., Coinbase) or user managed (e.g., MyEtherWallet).

Distributed ledger technology ("DLT"): often used interchangeably with the term *blockchain*, but while all blockchains are a type of DLT, not all DLTs implement a blockchain style of achieving consensus.

Fintech: new technology and innovation that aims to compete with traditional financial methods in the delivery of financial services.

Initial coin offering: a type of crowdfunding using cryptocurrencies in which a quantity of the crowdfunded cryptocurrency is sold to either investors or consumers, or both, in the form of "tokens".

Initial token offering: *see* **Initial coin offering**.

Internet of Things: a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Licences, software: the grant of a right to use otherwise copyrighted code, including, among others:

- Apache.
- GPLv3.
- MIT.

Mining, cryptocurrency: the process by which transactions are verified and added to the public ledger known as the blockchain, which is often the means through which new units of a virtual currency are created (e.g., Bitcoin).

Money transmitter (U.S.): a business entity that provides money transfer services or payment instruments.

Permissioned network: a blockchain in which the network owner(s) decides who can join the network and issue credentials necessary to access the network.

Platform or protocol coins: the native virtual currencies transferable on a blockchain network, which exist as a function of the protocol's code base.

Private key: an alphanumeric cryptographic key that is generated in pairs with a corresponding public key. One can verify possession of a private key that corresponds to its public key counterpart without exposing it. It is not possible, however, to derive the private key from the public key.

Private key storage:

- *Deep cold storage*: a type of cold storage where not only Bitcoins are stored offline, but also the system that holds the Bitcoins is never online or connected to any kind of network.
- *Hardware wallet*: an electronic device capable of running software necessary to store private keys in a secure, encrypted state and structure transactions capable of being broadcast on one or more blockchain networks. Two popular examples are Ledger and Trezor.

Protocols: specific code bases implementing a particular blockchain network, such as:

- Bitcoin.
- R3's Corda.
- Ethereum.
- Hyperledger Fabric.
- Litecoin.

Public network: blockchain that anyone can join by installing client software on a computer with an internet connection. Best known public networks are Bitcoin and Ethereum.

Qualified custodian: a regulated custodian who provides clients with segregated accounts and often places coins or tokens in cold storage (*see above*).

Robo-advice/digital advice: a class of financial adviser that provides financial advice or investment management online, with moderate to minimal human intervention.

Sandbox (regulatory): a programme implemented by a regulatory agency that permits innovative start-ups to engage in certain activities that might otherwise require licensing with one or more governmental agencies.

Security token: a token intended to confer rights typically associated with a security (e.g., stock or bond), and hence, are generally treated as such by regulators.

Smart contract: a piece of code that is written for execution within a blockchain runtime environment. Such programmes are often written to automate certain actions on the network, such as the transfer of virtual currency if certain conditions in the code are met.

Tokens: a data structure capable of being fungible (ERC-20) or non-fungible (ERC-721) that is capable of being controlled by a person to the exclusion of others, which is typically transferable from one person to another on a blockchain network.

Utility token: a token intended to entitle the holder to consume some good or service offered through a decentralised application ("dApp").

Vending machine (Bitcoin): an internet machine that allows a person to exchange Bitcoins and cash. Some Bitcoin ATMs offer bi-directional functionality, enabling both the purchase of Bitcoin as well as the redemption of Bitcoin for cash.

Cryptocurrency compliance and risks: A European KYC/AML perspective

Fedor Poskriakov, Maria Chiriaeva & Christophe Cavin
Lenz & Staehelin

Introduction

The rapid development, increased functionality, and growing adoption of new technologies and related payment products and services globally continue to pose significant challenges for regulators and private sector institutions in ensuring that these technologies are not misused for money laundering ("**ML**") and financing of terrorism ("**FT**") purposes. The underlying reasons for this are numerous and some of such risks were identified and discussed already in 2013 in the Financial Action Task Force ("**FATF**") NPPS Guidance,[1] even though the said report did not specifically refer to "virtual currencies" at the time.

In the last couple of years, a significant number of virtual currencies and other virtual assets ("**VAs**") have emerged and at least some of them attracted significant investment in payment infrastructures built on the relevant software protocols. These payment infrastructures and protocols seek to provide a new method for transmitting value over the internet or through decentralised peer-to-peer networks.

As decentralised, convertible cryptography-based VAs and related payment systems are gaining momentum, regulators and financial institutions ("**FIs**") around the world are recognising that VAs and the underlying consensus protocols (1) likely represent the future for payment systems, (2) provide an ever-more powerful new tool for criminals, terrorist financiers and other sanctions-evaders to move and store illicit funds, out of the reach of law enforcement, and, as a result, (3) create unique new challenges in terms of ML/FT risks.[2] Although the global volumes and estimates are relatively low, Europol estimated in 2017 that 3–4% of Europe's crime proceeds were laundered through cryptocurrencies – the proportion will likely continue to increase rapidly[3] due to the rate of adoption of VAs, including by institutional investors and FIs.

Given the trans-jurisdictional (or borderless) nature of the VA phenomenon, major institutions at the international level have all focused on and issued reports addressing VAs and the risks associated with them, including ML/FT risks. FATF and the European Banking Authority ("**EBA**"), in particular, have issued recommendations in this context, concluding that VA exchange platforms allowing the conversion of VAs into fiat money (and *vice versa*) are of particular relevance and must be brought within the scope of the respective national anti-money laundering and counter-financing of terrorism ("**AML/CFT**") frameworks. In June 2019, FATF adopted changes to its Recommendations to explicitly clarify that they apply to financial activities involving VAs and certain virtual asset service providers ("**VASPs**"). More recently, FATF concluded that the revised standards on AML/CFT designed to specifically address VAs also apply to stablecoins.

Key potential risks

Key definitions and concepts

(a) *Definitions*

There is no single global definition of the term "crypto- or virtual currency". In 2012, the European Central Bank ("**ECB**") defined virtual currencies as "*a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community*".[4] In 2014, the EBA defined virtual currencies as a "*digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a [fiat currency], but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically*".[5] In its 2014 report on key definitions on virtual currencies, FATF first gave the following definition: "*[T]he digital representation of value that can be digitally traded and functions as: (i) a medium of exchange; and/or (ii) a unit of account; and/or (iii) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.*"

In order to provide for a common regulatory approach through the fifth Anti-Money Laundering Directive ("**MLD5**", see also "Current legal and regulatory regime, MLD5", below), the EU decided to adopt a definition of virtual currencies deriving from FATF's 2014 guidance. According to MLD5, a virtual currency is defined as a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange, and which can be transferred, stored and traded electronically. Given the broad nature of this definition, it is likely that, in practice, most forms of VAs and other transferable cryptographic coins or tokens (as we know them today) fall within the scope of MLD5.

Finally, FATF updated its Recommendations in October 2018 and introduced the definition of VAs, now defined as a "*digital representation of value that can be physically traded, or transferred, and can be used for payment or investment purposes*" (but do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations).[6] In its June 2020 report on stablecoins, FATF further concluded that stablecoins could either be classified as VAs or traditional financial assets under the revised FATF standards.[7]

For the purposes of this chapter, we will adopt the definitions and conceptual framework set out in FATF's updated Recommendations.[8] In this respect, we will focus on decentralised convertible VAs and related payment products and services ("**VCPPS**"), to the exclusion of other VA-related securities and/or derivatives products and services, even though these are also relevant for ML/FT risk assessment, in particular crowdfunding methods like initial coin offerings ("**ICOs**").

(b) *KYC and transaction monitoring*

Know Your Customer ("**KYC**") is the cornerstone of the AML/CFT due diligence requirements that are generally imposed on FIs whose AML/CFT legislation is aligned with international standards. KYC requirements are relatively recent, as they were first implemented in the 70s in both Swiss and US legislation, before becoming an internationally recognised concept through the issuance of the FATF Recommendations. KYC requires that FIs duly identify (and verify) their contracting parties (i.e.,

customers) and the beneficial owners (namely when their contracting parties are not natural persons) of such assets, as well as their origin. Together with transaction monitoring, KYC ensures the traceability of assets, as long as those remaining in the financial system (i.e., paper trail), and allows the identification of ML/FT indicia.

Although KYC and transaction-monitoring requirements were globally implemented at a time when VAs did not exist, it appears today, based on the various initiatives both at the international and national levels, that the application of AML/CFT requirements to VCPPS remains to be clarified.

One of the challenges is that KYC and other AML/CFT requirements were designed for a centralised intermediated financial system, in which regulatory requirements and sanctions can be imposed by each jurisdiction at the level of financial intermediaries operating on its territory (i.e., acting as "gatekeepers"). By contrast, VCPPS rely on a set of decentralised cross-border virtual protocols and infrastructure elements, neither of which has a sufficient degree of control over or access to the underlying value (asset) and/or information, so that identifying a touchpoint for implementing and enforcing compliance with AML/CFT requirements is naturally challenging.

Potential AML/CFT risks

It has to be recognised that like any money-transmitting or payment services, VCPPS have legitimate uses, with prominent venture capital firms investing in VA start-ups and developing infrastructure platforms. VAs may, for example, facilitate micro-payments, allowing businesses to monetise very low-cost goods or services sold on the internet. VAs may also facilitate international remittances and support financial inclusion in other ways, so that VCPPS may potentially serve the under- and un-banked.

However, most VAs by definition trigger a number of ML/FT risks due to their specific features, including anonymity (or pseudonymity), traceability and decentralisation. Many of those risks and uses materialise not on the distributed ledger ("**DL**") of the relevant VA, but rather in the surrounding ecosystem of issuers, exchangers and users. Rapidly evolving technology and the ease of new cryptocurrency creation are likely to continue to make it difficult for law enforcement and FIs alike to stay abreast of new criminal uses, so that integrating those in a solid KYC/client due diligence ("**CDD**") framework is a never-ending task.

In addition to potential illicit uses of VCPPS, the use of VAs may facilitate ML by relying on the same basic mechanisms as those used with fiat currency, with a significant potential for abuse of unregulated and decentralised borderless networks underpinning VAs. In a nutshell:

- **Placement**: VAs offer the ability to open a significant number of anonymous or pseudonymous wallets, at no or very low cost, something that is a low-risk method of rapidly placing proceeds of illicit activity.
- **Layering**: VAs enable the source of funds to be obfuscated by means of multiple transfers from wallet to wallet and/or their conversion into different types of VAs across borders. This allows for an easy layering without significant cost or risk, it being understood that recent technological developments such as "atomic swaps" may even further facilitate the misuse of VAs. Incidentally, substantial demand for unregistered ICOs may allow criminals (assuming they control the ICO) to hijack the popular crowdfunding mechanism to convert VA proceeds into other VAs and/or fiat currencies, while adding a seemingly legitimate "front" for the source of funds.
- **Integration**: the use of VAs to acquire goods or services, either directly or through the conversion of the VAs into fiat currency, is facilitated by the ever-increasing list of goods and services for which payment in VAs is accepted, as well as the entry into

the VA markets of institutional players both for investment and trading (speculation) purposes, providing substantial liquidity in the VA markets and thereby potentially facilitating large-scale integration by abusing unsuspecting institution actors/investors. Likewise, ICOs with below-average KYC requirements may be abused by criminal actors who may be able to convert their illicit VA holdings into other tokens through subscribing to an ICO, and then exiting the investment immediately upon the relevant coins or tokens becoming listed on any VA exchange.

Naturally, AML/CFT risks are heightened among the unregulated sectors of the cryptocurrency markets. Given regulatory pressure to reject anonymity and introduce AML controls wherever cryptocurrency markets interface with the traditional financial services sector, there are new VAs being created to be more compatible with existing regulations.

However, until such time as novel technological solutions are in place, ML/FT risks are typically addressed by imposing strict AML/KYC requirements on "gatekeepers" such as VA exchangers and other FIs. However, according to the Impact Assessment of the European Commission of July 2016,[9] depending on the evolution of the network of acceptance of VAs, there might come a point in time when there will no longer be a need to convert VAs back into fiat currency if VAs become widely accepted and used. This presents a critical challenge in itself, insofar as it will reduce the number of "touchpoints" (i.e., conversion points from VA to fiat, exchangers, etc.) with the traditional intermediated financial services sector and thereby limit the opportunities for ML/FT risk mitigation through regulation of defined intermediaries. The updated FATF Recommendations, however, significantly extended the scope of entities subject to AML/CFT regulation by ensuring that not only VA activities that intersect with and provide gateways to and from the traditional regulated financial system (in particular VA exchangers), but also crypto-to-crypto exchange platforms, ICO issuers, custodial wallets and other related service providers, are regulated for AML/CFT purposes (see "Current international initiatives, FATF", below).

Anonymity/pseudonymity

By definition, decentralised systems are particularly vulnerable to anonymity risks. Indeed, in contrast to traditional financial services, VA users' identities are generally unknown, although in most cases they are only pseudonymous, and there is no regulated intermediary that may serve as "gatekeeper" for mitigation of ML/FT risks.

The majority of VAs, such as *Bitcoin* ("***BTC***") or *Ether* ("***ETH***"), have anonymity or pseudonymity by design. The user's identity is not linked to a certain wallet or transaction. However, while a user's identity is not visible on the relevant DL underpinning the VA infrastructure, information on transactions, such as dates, value and the counterparties' addresses, are publicly recorded and available to anyone. For the purposes of their investigation and prosecution work, enforcement authorities are therefore able to track transactions to a point where the identity may have been linked to an account or address (e.g., wallet providers or exchange platforms).

Some VAs, such as Dash, Monero or Zcash and other "privacy coins", even go further, as they are designed to be completely anonymous: wallet addresses, transactions and information on transactions are not publicly recorded on the relevant DL and provide for complete anonymity, preventing the identification of the legal and beneficial owner of the VAs.

In addition, a number of solutions have emerged that allow a certain enhancement of the anonymity and seek to limit traceability of transactions on otherwise pseudonymous VA networks. For instance, mixing services (also known as "*tumblers*" or "*washers*") aggregate transactions from numerous users and enable the actual paper trail of the transactional

activity to be obscured. However, while the precise trail of individual transactions might be obscured, the fact that mixing activity has occurred is detectable on the relevant DL.

Traceability

Although the anonymous or pseudo-anonymous design of VAs is an obvious risk of ML/FT, the public nature of the DL acts as a mitigant by offering a complete transaction trail. The DL is an immutable, auditable electronic record of transactions whose traceability may, however, be limited due to user anonymity and anonymising service providers that obfuscate the transaction chain (see also "Technological solutions?", below).

The traceability or "trail" risks may not be significant when dealing with a single DL or VA protocol. However, the situation becomes much more complex when considering cross-VA exchanges where it may not necessarily be possible to easily trace conversion transactions from one VA/DL to another, given that such tracing may require access to off-chain records of intermediaries or exchangers, which may be unregulated, and located in multiple jurisdictions. Likewise, with the emergence of technological solutions allowing for so-called "atomic swap", or atomic cross-chain trading, traceability will become an even greater challenge. In essence, it will allow users to cross-trade different VAs without relying on centralised parties or exchanges.

Decentralisation

Most VAs are decentralised, i.e., they are distributed on a peer-to-peer basis and there is no need for validation by a trusted third party that centrally administers the system. As noted by FATF, law enforcement cannot target one central location or entity (administrator) for investigative or asset-seizure purposes, and customers and transaction records are typically held by different parties, in multiple jurisdictions, making it more difficult for law enforcement and regulators to access them.[10]

This problem is exacerbated by the rapidly evolving nature of the underlying DL technology and VCPPS business models. Without proper safeguards in place, transition from a VCPPS to the fiat financial system may be facilitated by unsuspecting VA exchangers and/or abused by complicit VCPPS infrastructure providers who deliberately seek out jurisdictions with weak AML/CFT regimes or deficient implementation of related controls.

Legal and regulatory challenges

Current legal and regulatory regime

Despite calls for the adoption of global AML standards for VAs, no such uniform rules have yet emerged. However, we have seen some convergence toward the logical FATF view that VCPPS should be subject to the same obligations as their non-VA counterparts. In this respect, the majority of European jurisdictions that have issued rules or guidance on the matter have typically concluded that the exchange of VA for fiat currency (including the activity of VA "exchanges") is or should be subject to AML obligations.

Differences in national regulations include: (1) varying licensing requirements for VA exchangers and wallet services; (2) treatment of ICOs from an AML regulatory standpoint; and (3) the extent to which crypto-to-crypto exchange is treated differently from crypto-to-fiat exchange. In many cases, the regulatory status of these activities is either ambiguous or case-specific, and partially dependent on new legislation or regulation being adopted.

EU

VAs were first addressed at the EU level when the ECB published its VA report in October 2012. The ECB notably acknowledged that the degree of anonymity afforded by VAs can

present ML/FT risks. The ECB further suggested that regulation "would at least reduce the incentive for terrorists, criminals and money launderers to make use of these virtual currency schemes for illegal purposes".[11]

In July 2014, the EBA issued a formal opinion on VAs, indicating in particular that VAs present high risks to the financial integrity of the EU, notably due to potential ML/FT risks. In its January 2019 report,[12] however, the EBA noted that VA-related activity in the EU was regarded as relatively limited and that such activity does not appear to give rise to implications for financial stability.

MLD5

On July 5, 2016, the European Commission presented a legislative proposal to amend MLD4. The proposal was part of the Commission's Action Plan against FT, announced in February 2016. It also responded to the "Panama Papers"[13] revelations of April 2016.

MLD5 was adopted by the Parliament in plenary on April 19, 2018 and the Council of the European Union adopted it on May 14, 2018. It was formally published in the EU's *Office Journal* on June 19, 2018 and entered into force on July 9, 2018. Member States had until January 10, 2020 to amend their national laws to implement MLD5. To date, most Member States have fully implemented MLD5, although some of those failed to transpose MLD5 completely within the original prescribed deadlines.

Among different objectives, MLD5 expressly aims at tackling FT risks linked to VAs. In this context, VA exchange platforms and custodian wallet providers have been added in the scope of MLD5. In order to allow competent authorities to monitor suspicious transactions involving VAs, while preserving the innovative advances offered by such currencies, the European Commission concluded that it is appropriate to include in the institutions subject to MLD4 ("obliged entities") all gatekeepers that control access to VAs, and in particular, exchange platforms and wallet providers,[14] as recommended by FATF in its guidance (see "Current international initiatives, FATF", below).

(i) *Providers engaged in exchange services*
Interestingly, MLD5 extends EU AML requirements to "providers engaged in exchange services between virtual currencies and fiat currency". As a result, most crypto-to-fiat (or fiat-to-crypto) exchanges will be covered by MLD5. However, crypto-to-crypto exchanges do not seem to be expressly covered by MLD5.
Notwithstanding this, it is still possible that certain crypto-to-crypto exchanges may fall within the scope of MLD5 if their activities are conducted by "obliged entities" for other reasons, such as custodian wallet services (see (ii) below). Further, crypto-to-crypto exchanges could still be regulated at Member State level, depending on how each Member State incorporates MLD5's provisions into its national law, as well as the FATF Recommendations. Similarly, VA ATMs are not covered under MLD5, but some Member States have introduced more stringent rules that cover those activities.

(ii) *Custodian wallet providers*
Custodian wallet providers are defined entities that provide services to safeguard private cryptographic keys on behalf of customers, to hold, store and transfer VAs. The definition appears to only include wallet providers that maintain control (via a private cryptographic key) over customers' wallets and the assets in it, in contrast to pure software (non-custodial) wallet providers that provide applications or programs running on users' hardware (computer, smartphone, tablet, etc.) to access public information from a DL and access the network (without having access to or control over the user's private keys).

Switzerland

The Swiss AML legislation does not provide for a definition of VAs, relying upon FATF's definition used in its 2014 report. That being said, since the revision of the Swiss Financial Market Supervisory Authority ("**FINMA**") AML Ordinance in 2015, exchange activities in relation to VAs, such as money transmitting (i.e., money transmission with a conversion of VAs between two parties), are clearly subject to AML rules. Before this revision took place, both FINMA and the Federal Council had already identified,[15] on a risk-based approach, the increased risks associated with VA exchangers and the necessity for them to be subject to AML requirements. As such, Switzerland was a precursor in the implementation of this rule, which has now become standard.

In a nutshell, the purchase and sale of convertible VAs on a commercial basis, and the operation of trading platforms to transfer money or convertible VAs from a platform's users to other users, are subject to Swiss AML rules, including the so-called "travel rule". Before commencing operations, a provider of these kinds of services must become a member of a self-regulatory organisation ("**SRO**").

Because convertible VAs can facilitate anonymity and cross-border asset transfers, FINMA considers trading in it to have heightened ML/FT risks, requiring strict CDD, particularly as regards client identification, beneficial ownership and source-of-funds analysis.

The key AML/CFT compliance requirement, which represents a challenge to FIs providing VSPPS because of the very nature of currently existing VAs, is undoubtedly the "travel rule". This rule requires that information about the client and the beneficiary be transmitted with payment orders.[16] Although 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 a DL, there are practical ways for FIs to still comply with this requirement; however, they are comparatively onerous and therefore severely limit the development of VCPPS. Notwithstanding this, there are several industry initiatives that aim at developing a technical solution to reliable and standardised implementation of the "travel rule" requirements, such as OpenVASP or interVASP. Once some of those standards are vetted by AML regulators, it should be expected that more VCPPS will be offered on the market and that it will become easier to combine the purely decentralised world of VAs and traditional intermediated financial services.

Managing compliance AML/CFT risks

Although there are developments on the regulatory front in terms of strengthening requirements applicable to VCPPS providers, there has been little guidance by regulators to their respective domestic FIs as to how to approach KYC/CDD from an ML/FT risk assessment perspective when dealing with customers exposed to VA and VCPPS risks, other than a recommendation to adopt a prudent, risk-based approach.

In practice, as with any new line of business, type of client or financial transaction, the central AML/CFT compliance questions for FIs will be whether they: (1) understand the relevant risks; (2) can reasonably manage them; and (3) have the knowledge, tools and resources to do so on an ongoing basis (including policies, procedures, training programmes, etc.). FIs that choose to serve the new types of clients in the VA ecosystem should elaborate and put in place specific policies and procedures to ensure that they are able to comply with their AML obligations despite the VA context.

The specifics of each set of requirements will depend on the type of business, client type and jurisdiction, as well as other factors. That being said, the ability of FIs to confirm the identity,

jurisdiction and purpose of each customer, as well as the assessment of the source of wealth and funds, is essential to the fulfilment of AML/CFT requirements. VCPPS actors as customers present specific challenges in each of these aspects, so that FIs must ensure that their policies and procedures allow them to perform these core functions with a degree of confidence that is at least equal to that which FIs would require for their traditional financial services.

Given the varying typology of VCPPS service providers, it is virtually impossible to draw up KYC/CDD standards, procedures and checklists that would be applicable universally. It is therefore understandable that regulators have not issued blanket guidance in this space. As the understanding of VCPPS and related AML/CFT risks evolves, it is likely that international standards and recommendations will emerge, and possibly compliance tools which will simplify the implementation thereof by FIs. In this respect, FIs, VCPPS providers, developers, investors, and other actors in the VA space should seek to develop technology-based solutions that will improve compliance and facilitate the integration of VCPPS with the existing financial system.

Possible avenues to address compliance concerns

Current international initiatives

FATF

(a) Virtual Currencies – Guidance for a risk-based approach (June 2015 Standards)

In June 2015, FATF issued specific guidance on virtual currencies, focusing on the points of intersection that provide gateways to the regulated financial system – *Guidance for a Risk-Based Approach: Virtual Currencies* (the "**Guidance**"). This Guidance derives from previous reports of FATF, namely the June 2014 *Virtual Currencies Report* and the FATF NPPS Guidance of June 2013.

In accordance with the cardinal risk-based approach principle, the Guidance provides for a certain number of clarifications on the application of the FATF Recommendations to entities involved in VCPPS.

FATF is of the view that domestic entities providing convertible VA exchange services between VA and fiat currency should be subject to adequate AML/CFT regulation in their jurisdiction, like any other FI, and be subject to prudential supervision. In this context, the distinction between centralised and decentralised VAs is a key aspect for the purposes of the risk assessment to be performed. FATF recommends that entities involved in convertible and decentralised VCPPS be subject to an enhanced due diligence process, as such activities are regarded as higher risk due to the inherent anonymity element and challenges to perform proper identification (i.e., the underlying protocols on which the major part of the decentralised VCPPS are currently based do not provide for the participants' identification and verification) (see also "Anonymity/pseudonymity", above).

It is important to note that FATF does not recommend prohibiting VCPPS. On the contrary, such prohibition could drive such activities underground and lead to a complete lack of visibility and control over them. As a result, in case of prohibition of VCPPS, FATF recommends implementing additional mitigation measures, taking also into account the cross-border element in their activities.

As regards transaction monitoring, FATF is of the view that countries must ensure that originator and beneficial owner information is always included when convertible VA exchangers conduct convertible VA transfers in the form of wire transfers. Certain *de minimis* thresholds may, however, be implemented in order to exclude lower risk transactions. Transaction monitoring remains a key risk mitigant in the convertible VA world, as long as a conversion of VAs occurs.

(b) FATF Recommendations

FATF updated its Recommendations in October 2018 to address the rapidly evolving risks related to VAs and to clarify how the FATF Recommendations apply in the case of financial activities involving VAs. The updated Recommendations specifically address and target VASPs, defined as any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between VAs and fiat currencies; (ii) exchange between one or more forms of VAs; (iii) transfer of VAs; (iv) safekeeping and/or administration of VAs or instruments enabling control over VAs; and (v) participation in and provision of financial services related to an issuer's offer and/or sale of a VA.

These new definitions significantly expand the scope of entities subject to AML/CFT regulation since the June 2015 Guidance by ensuring that VASPs (not only fiat-to-VA exchanges but also crypto-to-crypto exchange platforms, ICO issuers, custodial wallets and other related service providers) are regulated for AML/CFT purposes, as well as licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. That being said, the above-mentioned definitions remain somewhat vague, and their interpretations remain to be determined.

(c) Interpretive Note to Recommendation 15

FATF adopted an Interpretive Note to Recommendation 15 on June 21, 2019, setting out requirements for effective regulation, supervision and monitoring of VASPs. Under this note, VASPs should be licensed or registered and be subject to effective regulation and supervision to ensure that they take the necessary steps to mitigate AML/CTF risks. To this end, VASPs should (1) be supervised or monitored by a competent authority (not a self-regulatory body), which should conduct risk-based supervision or monitoring and have power to impose a range of disciplinary and financial sanctions, and (2) adopt a number of preventive measures to mitigate ML and FT risks (including but not limited to CDD, record-keeping, suspicious transaction reporting and screening all transactions for compliance with targeted financial sanctions). In particular, VASPs should conduct CDD for occasional transactions above a USD/EUR 1,000 threshold. According to Paragraph 7(b) of the Interpretive Note, VASPs should obtain and hold required and accurate originator and beneficiary information in relation to VA transfers, and share this information with beneficiary VASPs and counterparts, as well as competent authorities (often referred to as the "travel rule"). Further, the specific requirements relating to wire transfers (such as monitoring the availability of information, taking freezing actions and prohibiting transactions with designated persons and entities) as set out under Recommendation 16 would apply on the same basis to transfers of VAs.

The Interpretative Note finally highlights the need for international cooperation and information exchange to prevent and combat ML/FT risks associated with VAs.

While the "travel rule" has been a longstanding requirement for FIs internationally, the implementation of this requirement for VASPs to collect and transfer customer information during transactions will undoubtedly present a challenge considering the very nature of DL technologies. Indeed, whereas FIs rely on established interbank communication systems (such as SWIFT, TARGET or SIC) to move funds and share information, no established communication system yet exists for VASPs, and DL technologies – as they stand – usually only require a recipient address to effect a transfer, which renders difficult – if not impossible – ownership verification by VASPs and determination of whether the recipient address is managed by another obliged VASP or a non-custodial wallet which would fall outside the FATF Recommendations.

(d) Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019 Standards)
In June 2019, FATF published the *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, which builds upon FATF's June 2015 Standards on the risk-based approach to VAs and VASPs and is intended to help both national authorities in understanding and developing regulatory and supervisory responses to VA activities and VASPs, as well as to help VASPs in understanding their AML/CFT obligations. Under the risk-based approach and in accordance with Paragraph 2 of the Interpretative Note, countries should identify, assess, and understand the ML/FT risks in relation to VA financial activities or operations and VASPs and focus their AML/CFT efforts on potentially higher-risk VAs. Similarly, countries should require VASPs to identify, assess, and understand the ML/FT risks. Finally, in a report dated June 2020, FATF confirmed that the June 2019 Standards also apply to stablecoins, as they are to be considered either VAs or traditional financial assets depending on their exact nature. In particular, entities involved in any stablecoins might have AML/CFT obligations, depending on the activities these entities undertake (i.e., an activity of an FI or that of a VASP) and the design of the stablecoin (a key element being the extent to which the stablecoin arrangement is centralised or decentralised).

(e) Implementation monitoring of the June 2019 Standards
FATF completed in early July 2020 a review of the implementation of its June 2019 Standards on VAs and VASPs. FATF found that both the public and private sectors have generally made progress in implementing the revised FATF standards. FATF was advised that 35 out of 54 reporting jurisdictions have implemented the June 2019 Standards, with 32 of these regulating VASPs and three of these prohibiting the operation of VASPs, whilst the other 19 jurisdictions have not yet implemented the revised standards into national law. FATF further noted some progress in the supervision of VASPs and the implementation of AML/CFT obligations by VASPs (although generally still nascent). Progress in the development of technological solutions to enable the implementation of the "travel rule" was noted, although issues remain to be addressed by the public and private sectors for a practical implementation of the recommendations.
Considering that the VAs sector is fast-moving and technologically dynamic, FATF decided to (i) continue its enhanced monitoring of VAs and VASPs and undertook a second 12-month review of the implementation of the revised FATF standards on VAs and VASPs by June 2021, (ii) release updated Guidance on VAs and VASPs, (iii) continue to promote the understanding of AML/FT risks by publishing red flag indicators and relevant case studies, (iv) continue and enhance its engagement with the private sector, and (v) continue its programme of work to enhance international cooperation amongst VASP supervisors.

Latest discussions and developments

G-20

In its communication of June 8 and 9, 2019, the G-20 reaffirmed its commitment to applying the recently amended FATF standards to VAs and related service providers for AML/FT purposes. It is likely that essentially the G-20 will continue to rely upon FATF's position to ensure that global solutions are implemented at a broader level (through the 37 FATF Member States and the nine FATF-Style Regional Bodies). Further, in October 2019, the G-20 asked FATF to consider the AML/CFT issues relating to stablecoins, which was addressed in FATF's June 2020 report.

Bank of International Settlement

In its statement on VAs of March 2019, the Bank of International Settlement ("**BIS**") recalled that VAs have exhibited a high degree of volatility and are considered an immature asset class given the lack of standardisation and constant evolution. In this respect, the BIS highlighted the various risks that VAs present for banks, including AML/CFT risks, but also liquidity, credit, market, operational, legal and reputation risks. Accordingly, the Basel Committee set out its prudential expectations related to banks' exposures to VAs and related services that banks must at a minimum adopt (such as conducting comprehensive analyses of the risks noted above, implementing a clear and robust risk management framework that is appropriate for the risks of VA exposures and related services). According to BIS Paper No. 107 dated January 2020, however, no central bank reported any significant or wide public use of VAs for either domestic or cross-border payments, and the usage of VAs was considered either minimal or concentrated in niche groups.

UK

It is worth noting that in July 2020, the UK's Joint Money Laundering Steering Group ("**JMLSG**") updated its sectorial guidance on the AML regime applicable to UK firms active in the VA industry. The guidance provides for practical support in the implementation of AML requirements and lists the factors that may increase AML risks in the VA sector. Once approved by HM Treasury, the guidance will be used by the Financial Conduct Authority ("**FCA**") in its assessment of potential breaches of AML regulations by VA firms.

Creation of specific Financial Intelligence Units

The creation of specific Financial Intelligence Units ("**FIUs**") for VA-related transactions could be one of the measures to be implemented at national level that would have an impact at the international level. The cooperation between such specific FIUs would improve investigatory assistance and international cooperation in this respect (as stated in the Guidance).

Self-regulation and codes of conduct

Like Switzerland, certain jurisdictions attach great importance to self-regulation in the context of AML/CFT. Specific codes of conduct and self-regulations issued by SROs monitoring the compliance of affiliated FIs may be one of the measures that could be taken to address the ML/FT issue in relation to VAs quickly and efficiently. FIs active in the sector of cryptocurrencies, such as VA exchangers, could be specifically targeted by self-regulations adapted to their activities and providing for more clarity on their KYC and due diligence duties. Regulators and/or legislators could issue general guidelines and principles in this area, while specialised SROs could enrich them with detailed and practical recommendations until a consensus is found at the international level.

Central bank cryptocurrencies

Based on the various statements and reports on VAs issued by central banks in different jurisdictions, it appears that central banks agree that VAs such as *BTC* and *ETH* are not meant to replace fiat currency. According to the *International Monetary Fund Global Financial Stability Report* dated April 2018, the use of cryptocurrencies as a medium of exchange has been limited and their high volatility has prevented them from becoming a reliable unit of account. In this context, VAs do not appear to pose macro-critical financial stability risks at present, although if widely used, they may raise issues about, *inter alia*, ML and investor and consumer protection.

Notwithstanding the above, some 80% of central banks (such as Banque de France, Norges Bank and the Bank of England) are currently following the evolution of the developments of VAs and central bank cryptocurrencies (the "**CBCCs**") closely or even contemplating

issuing their own CBCC in order to take advantage of the dematerialisation of the currency (triggering costs reductions) and to facilitate international transactions by avoiding currency exchanges issues and providing for instantaneous transfers, security and monitoring capabilities according to BIS Paper No. 107 dated January 2020.

CBCCs could be viewed as a solution to mitigate the ML/FT risks, as the transactions related thereto would necessarily go through a regulated financial intermediary subject to AML/CFT regulations. This presupposes a new generation of centralised cryptocurrencies which will not have the same level of anonymity and transferability as the current cryptocurrencies. In this respect, it is worth noting that the BIS indicated in its March 2018 report, *Central bank digital currencies*, that the issuance of CBCCs could come, in addition to more efficient and safer payments and settlement systems, with some benefits from an AML/CFT perspective. To the extent that CBCCs allow for digital records and traces, it could indeed improve the application of rules aimed at AML/CFT, as well as reduce costs of compliance. To date, we are not aware of central banks having issued their own CBCCs (with the exception of the specific case of Venezuela which has issued a state cryptocurrency backed by the country's oil and mineral reserves (i.e., the petro)).

In this context, in some part as a reaction to Facebook's Libra project and also in response to China's plans in the field of digital currencies and payments, a growing demand is forming for some form of programmable digital money which can be integrated into the existing financial system. Indeed, the potential of technology is self-evident – a national currency which is fully programmable becomes *de facto* resilient to ML/FT risks by design and would discourage non-compliant uses of such currency. However, the various risks and legitimate privacy concerns need to be addressed before such a means of payment becomes socially acceptable or desirable.

Technological solutions?

According to certain authors and actors active in the cryptocurrency field, the specific features of DL technologies and protocols could be used to mitigate the ML/FT risks in relation to VAs. KYC, beneficial owner and transactional information could be registered and verified on a dedicated DL, in the form of a global network of unalterable information (or global data repository) that would be accessible by "gatekeepers" and law enforcement. This solution, although very promising at first sight, would raise significant technical and legal issues. Among the latter, one should mention the legal requirements in terms of data protection and, as the case may be, banking secrecy. Furthermore, the access to information and its use by public authorities, such as criminal prosecution authorities, would have to be strictly regulated in order to avoid any intervention outside the applicable mutual assistance channels. In this respect, and as one of the main challenges, such a private DL would need to comply with rules enacted at an international level by the jurisdictions whose FIs would be involved in such network. It appears, therefore, that there are a certain number of obstacles as of today to using DL technologies for AML/CFT purposes, especially in the absence, at this stage, of clear guidance and standards at the international level.

As mentioned in the FATF 2015 report on VAs, other technical solutions may be available. Third-party digital identity systems, as well as new business models, could be developed to facilitate customer identification/verification, transaction monitoring and other due diligence requirements. In particular, in FATF's view, application programming interfaces ("**API**") that provide customer identification information, or allow FIs to set conditions

that must be satisfied before a VA transaction can be sent to the recipient, could be used to reduce the ML/FT risks associated with a VCPPS. A certain number of fintech companies have already started to develop technological AML solutions.

Conclusion

VCPPS continue to gain momentum. As adoption increases and innovation relevant to AML/CFT compliance becomes embedded in the VCPPS "genetics", we may witness the emergence of improved existing VA protocols or entirely new VAs, built on fundamentally different underlying principles that could include built-in controls, trusted "gatekeepers", digital identity interfaces and transaction monitoring.

Unfortunately, for as long as consistent and recognised standards and/or compliance tools are lacking, many legitimate actors in the VCPPS space will continue to be denied access to traditional banking services in a number of jurisdictions, and/or be "de-risked" by FIs. To the extent that international standard-setters, national regulators, FIs and VCPPS service providers and innovators recognise the opportunities and benefits of VCPPS globally, they should cooperate to define best practices and open, interoperable standards (as opposed to proprietary solutions), as well as training programmes for the next generation of VA "compliance officers". Indeed, applying existing concepts and approaches tailored to an intermediated, centralised financial infrastructure simply does not work when transposed to VA ecosystems which abide by different rules and principles by design.

* * *

Endnotes

1. *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, June 2013, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.
2. Communication from the Commission of the European Parliament and of the Council on an Action Plan for strengthening the fight against FT, Strasbourg, February 2, 2016.
3. Europol, *Drugs and the Darknet – Perspectives for Enforcement*, 2017.
4. European Central Bank, *Virtual Currency Schemes*, October 2012.
5. European Banking Authority, *Opinion on virtual currencies*, July 4, 2014.
6. *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.
7. FATF, Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins, June 2020, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf.
8. Available here: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.
9. Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of ML or FT and amending Directive 2009/101/EC, July 5, 2016 ("**MLD4**").
10. FATF, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, June 2014.
11. Report of the ECB on Virtual Currency Schemes, October 2012.

12. European Banking Authority, *Report with advice for the European Commission on Crypto-assets*, January 9, 2019, https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf.
13. The documents, some dating back to the 1970s, were created by, and taken from, Panamanian law firm and corporate service provider Mossack Fonseca, and were leaked by an anonymous source.
14. European Commission, *Explanatory Memorandum*, proposal for a Directive of the European Parliament and of the Council amending MLD4.
15. Swiss Federal Council Report on Virtual Currencies, June 25, 2014.
16. FINMA Guidance 02/2019 – Payments on the blockchain, August 26, 2019.

Fedor Poskriakov
Tel: +41 58 450 7131 / Email: fedor.poskriakov@lenzstaehelin.com
Fedor Poskriakov is a partner at Lenz & Staehelin in the Banking and Regulatory group in Geneva and specialises in banking, securities and finance law. He regularly advises on various regulatory, contractual and corporate matters. His practice covers banking, investment management and alternative investments, including private equity and hedge funds. He also heads the firm's Geneva office fintech practice. Highlighted as a "Next Generation Lawyer" (*The Legal 500*, 2019), Fedor Poskriakov is recognised for his "impressive expertise in the Fintech space" (*Who's Who Legal*, 2019) and "his great understating of the blockchain technology itself, combined with his concrete experience in translating this into practice" (*Chambers*, 2019).

Maria Chiriaeva
Tel: +41 58 450 7000 / Email: maria.chiriaeva@lenzstaehelin.com
Maria Chiriaeva is a senior associate in the Banking and Finance and the Investigations groups in Geneva and specialises in banking, securities and finance law. She regularly advises on various regulatory, contractual and corporate matters. Her practice covers banking, investment management and alternative investments. Her areas of expertise also include compliance advisory and internal investigations. Maria Chiriaeva is admitted to the Bar in Geneva. She has a Master's in economic law from the University of Geneva.

Christophe Cavin
Tel: +41 58 450 7000 / Email: christophe.cavin@lenzstaehelin.com
Christophe Cavin is a senior associate in the Geneva office and is a member of the Banking and Finance group and the Investigations group, respectively. His main areas of practice include banking and finance, regulatory, investigations, corporate, commercial and contractual matters. Christophe Cavin is admitted to the Bar in Geneva and New York. He has a Master's in commercial law from the University of Geneva and an LL.M. from the University of Pennsylvania Law School.

Lenz & Staehelin

Route de Chêne 30, CH-1211 Geneva 6 / Brandschenkenstrasse 24, CH-8027 Zurich, Switzerland
Tel: +41 58 450 7000 / +41 58 450 8000 / Fax: +41 58 450 7001 / +41 58 450 8001 / URL: www.lenzstaehelin.com

www.globallegalinsights.com

Other titles in the **Global Legal Insights** series include:

AI, Machine Learning & Big Data
Banking Regulation
Bribery & Corruption
Cartels
Corporate Tax
Employment & Labour Law
Energy
Fintech
Fund Finance
Initial Public Offerings
International Arbitration
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Pricing & Reimbursement

GLI GLOBAL LEGAL INSIGHTS