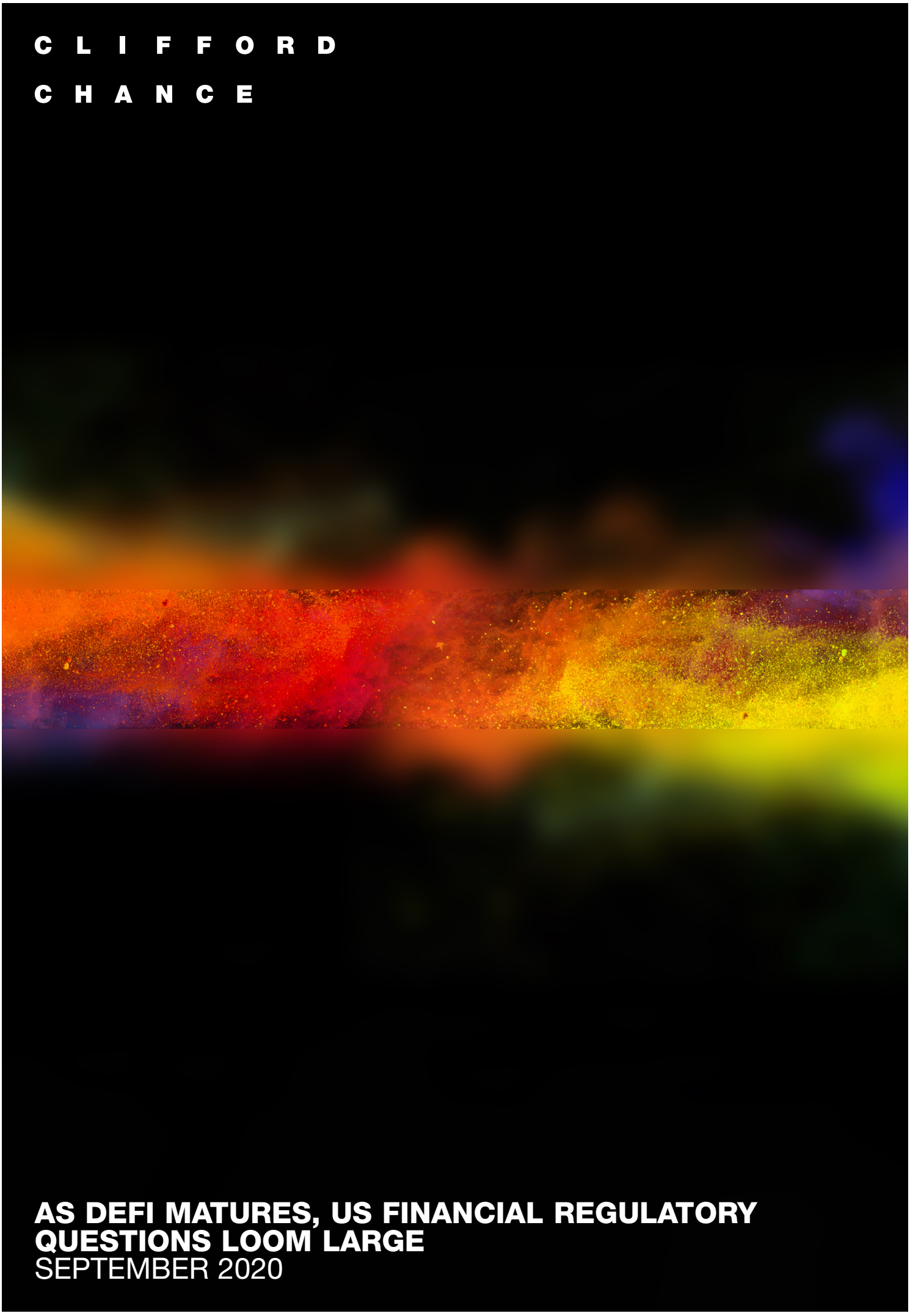
CLIFFORD

CHANCE



AS DEFI MATURES, US FINANCIAL REGULATORY QUESTIONS LOOM LARGE

SEPTEMBER 2020

AS DEFI MATURES, US FINANCIAL REGULATORY QUESTIONS LOOM LARGE

The decentralized finance or "DeFi" movement aspires to create a global peer-to-peer alternative to traditional financial services using permissionless distributed ledger or blockchain technology. DeFi companies have reportedly taken in billions in cryptocurrency over recent months, with some estimates placing the total amount currently "locked" in DeFi-related platforms at almost $8 billion.[1] But financial services offered by global DeFi platforms could be subject to relevant local laws and regulations that may, if not adhered to, present regulatory enforcement risks for DeFi providers.

In the US, the US Securities and Exchange Commission (SEC) and US Commodity Futures Trading Commission (CFTC) recently took enforcement action for violations of the US securities laws and the Commodity Exchange Act against entities doing business as "Abra" which developed a blockchain-based smart contracts app advertised as a DeFi platform that provided users with synthetic investment exposure to various assets through swap contracts. DeFi platforms may also attract scrutiny from the US Treasury's Financial Crimes Enforcement Network (FinCEN), because many allow users to transmit and/or exchange virtual currencies. FinCEN has made statements this year about ensuring compliance with its registration and other regulatory requirements – particularly with respect to non-US platforms on which US persons can transact in virtual currencies. Although to date, nascent DeFi platforms seem to have avoided publicized US regulatory scrutiny, this may change if platforms continue attracting significant capital, particularly from retail users.

In this article, we explore what DeFi is, review the recent SEC and CFTC actions against Abra, explore some of the red flags that DeFi platforms should be aware of and discuss steps that platforms can take to avoid inadvertently violating US regulatory requirements.

1. Total Value Locked (USD) in DeFi Chart available at **https://defipulse.com/** (September 2020). While the calculation methodology and accuracy of the defipulse.com numbers are unclear, Total Value Locked or TVL is a metric that, if accurate, can be used to assess the DeFi growth rate and overall health of DeFi platforms. Many prominent DeFi platforms require users to contribute and essentially "lock" digital assets like bitcoin (BTC) or Ether (ETH) into smart contracts for a period of time as collateral for loans or in exchange for other digital assets, interest payments, etc. True to its name, TVL measures the total USD value of digital assets currently locked in DeFi smart contracts as calculated by the defipulse.com website.

What is DeFi?

No universally accepted definition of DeFi has emerged, but, broadly speaking, DeFi seeks to leverage the power of distributed ledger or blockchain technology to create a global, decentralized, and widely accessible alternative to regulated financial services including lending, payments, spot and financial derivatives trading, market making, and wallet/account provision. While DeFi developers strive for decentralized governance, project development, and true peer-to-peer transactions, their projects often require more centralized management and development at inception and in earlier stages of development. No DeFi platform seems to have achieved true decentralization yet, such as that of Bitcoin. For now, the "decentralized" in DeFi seems to refer more to an aspiration for future decentralization, or to the use of decentralized blockchain protocols like Ethereum and their smart contract capabilities to create easily accessible alternatives to traditional financial institutions.

Functionally, many DeFi platforms appear to offer financial services that may be subject to financial services regulation, with many popular platforms appearing to combine multiple financial services. For example, platforms that facilitate so-called "yield farming" allow users to open wallets/accounts, and incentivize users to lend digital assets like ETH to an asset pool in exchange for earning interest on the "locked" assets. The interest typically comprises a percentage of the market making fees generated by traders on the platform who utilize the asset pool for liquidity, and/or newly minted tokens distributed by the platform that can also be traded by users. This is made possible through decentralized applications or DApps created by platform developers using smart contracts on Ethereum or other blockchain protocols. Users often access the platform and its DApps through more traditional smartphone apps, meaning that DeFi platforms can be used by anyone in the world with a smartphone and internet connection.

The SEC & CFTC take action against Abra

The SEC and CFTC recently settled parallel enforcement actions against Plutus Financial, Inc., the US-based developer of a DeFi app called Abra (Abra US), and its Philippines-based affiliate, Plutus Technologies Philippines Corporation (Abra Philippines, and, together with Abra US, Abra).[2]

According to the settlement orders, Abra users first downloaded a smartphone app to link them with Abra's blockchain-based DApps (the App). After downloading the App, users created a user-controlled Abra wallet and funded it with BTC or other assets that Abra would convert into BTC (eg, Litecoin, ETH, or fiat currency). The US regulators alleged that Abra's onboarding process did not subject users to minimum asset or net worth thresholds or other sophistication or other eligibility screening. The orders also stated that Abra did not initially subject users who funded their accounts with digital assets to anti-money laundering (AML), know your customer (KYC) or sanctions screening. Instead, the orders alleged that Abra only collected users' IP addresses, email addresses, and, in some cases, phone numbers. The SEC alleged that Abra's lack of AML/KYC procedures resulted in it not knowing the identities of more than 20,000 users who signed up in early 2019.

2. *In re: Plutus Financial Inc., d/b/a Abra and Plutus Technologies Philippines Corp., SEC Rel. No. 34-89296 (July 13, 2020) available at* **https://www.sec.gov/litigation/admin/2020/33-10801.pdf**; *In the Matter of: Plutus Financial, Inc. (d/b/a Abra) and Plutus Technologies Philippines Corp. (d/b/a Abra International),* CFTC Docket No. 20-23 (July 13, 2020) available at **https://www.cftc.gov/PressRoom/PressReleases/8201-20**.

According to the orders, users could enter "crypto-collateralized contracts" with Abra (the Abra Contracts) through the App after signing up and funding their wallets. Abra Contracts provided users with synthetic exposure to a variety of Reference Assets, which included US public-company stocks and exchange-traded funds (ETFs), fiat currencies, and virtual currencies. Abra was the counterparty to users' Abra Contracts and purchased and sold Reference Assets for its own account to hedge its exposure under the Abra Contracts. Each Abra Contract was memorialized in a "smart contract" on the Bitcoin blockchain and had a 25-day term. If the Reference Asset underlying the Abra Contract appreciated in value by the end of the term, the smart contract automatically returned the user's initial BTC deposit plus additional BTC in the amount of the increase. If the Reference Asset's value fell, the smart contract deducted the value of the decrease from the user's BTC deposit and returned the remainder. Users never owned or took possession of Reference Assets.

According to the settlement documents, in February 2019, the SEC and CFTC jointly contacted Abra and warned that its provision of Abra Contracts to US persons violated US laws regulating swap transactions. The regulators claimed regulatory jurisdiction over Abra because the Abra Contracts operated like contracts for difference or CFDs (a form of swap contract to exchange the difference in value of an underlying asset between the time at which a CFD position is established and the time at which it is terminated). Specifically, the SEC claimed regulatory jurisdiction over Abra because some Abra Contracts derived value from Reference Assets that are securities (eg, US public company stocks and ETFs), making them Security-Based Swaps[3]. The CFTC asserted regulatory jurisdiction because other Abra Contracts had fiat currencies or virtual currencies as the Reference Assets and thus qualified as Swaps, subject to CFTC's jurisdiction.

The orders describe Abra's efforts to mitigate its exposure to US regulation by, among other things: (i) monitoring user IP addresses, phone numbers, and the bank account locations of those who used fiat currency, to screen out US persons; (ii) drafting a new agreement under which users entered into Abra Contracts with Abra's non-US affiliate Abra Philippines instead of Abra US; (iii) using Asia-based servers to help run the App; and (iv) trying to code the Abra website to only show non-US persons pages related to Security-Based Swaps and Swaps.

The SEC alleged in its order that Abra's steps were insufficient because Abra US employees still played key roles in the overall business, including: (i) designing the swaps; (ii) designing marketing campaigns and directly participating in marketing activities; (iii) assisting with user AML/KYC; and (iv) executing hedging strategies. The SEC also alleged that Abra's approach of monitoring user phone numbers, IP addresses, and the location of their bank accounts, still failed to prevent the sale of around seven Security-Based Swaps to five US persons.

The CFTC similarly alleged that Abra remained subject to CFTC regulation even after ceasing to transact with US persons because Abra US employees designed and established the hedging mechanism for the Abra Contracts, prepared Abra marketing materials, and provided technical support and accounting services. Despite Abra's

3. DeFi platforms must also consider the "security" status of any tokens that can be traded/exchanged on their platforms and of any tokens issued by the platform itself. Whether a digital asset is a security depends on its specific characteristics and the economic rights it represents, and is beyond the scope of this note.

efforts, the SEC and CFTC assessed separate penalties in their respective enforcement actions totaling $300,000.[4]

FinCEN considerations

Regulatory obligations can attach to DeFi platforms even in the absence of transactions in SEC-regulated securities or Security-Based Swaps and/or CFTC-regulated instruments like Swaps. DeFi platforms generally rely on the use and/or deposit of virtual currencies like BTC or ETH and promote trading on the platform using the liquidity created by depositors. Some platforms also create and distribute their own coins to reward users. Entities that facilitate transactions in "convertible virtual currencies" for US customers generally must register with the Financial Crimes Enforcement Network or FinCEN, a bureau of the US Treasury Department, as money services businesses or MSBs."[5] The fact that a platform is "decentralized" does not exempt it from regulation.

FinCEN defines the term "virtual currency" broadly as a "medium of exchange that can operate like currency, but does not have all the attributes of 'real' currency . . . including legal tender status."[6] One type of virtual currency subject to FinCEN's jurisdiction is "convertible virtual currency" (CVC), which either has an equivalent value in real currency or acts as a substitute for real currency. FinCEN considers most established virtual currencies to be CVCs. Thus, the ETH, BTC, stablecoins, and many other virtual assets used, exchanged, and/or created on DeFi platforms are CVC.

FinCEN takes the position in its 2019 guidance that CVC issuers generally must register as MSBs, because at the time of issuance they are the only person authorized to issue and redeem the new units of CVC. This remains true even if the issuer, through contract or otherwise, declines to exercise its authority. Therefore, DeFi platforms that create their own virtual currencies may have FinCEN registration obligations and be required to adopt KYC and AML programs, designed to detect and prevent money laundering.

FinCEN's 2019 guidance also states that DApp owners/operators whose smart contracts "facilitate the exchange of CVC for currency or other CVC" likely qualify as money transmitters, regardless of whether they operate for profit. DeFi platforms that maintain wallets for their users, or that execute user transactions on a principal or riskless principal basis, are also likely to have FinCEN registration obligations and be required to adopt AML/KYC programs. DeFi platforms may also need to confirm that

4. The SEC and CFTC actions against Abra are not their first set of coordinated actions against a non-US software developer and trading platform for facilitating crypto-enabled derivatives transactions. That distinction belongs to 1Broker, based in the Marshall Islands, and its developer, chief executive, and owner Patrick Brunner, a resident of Austria. Unlike Abra, 1Broker had no US operations. Its platform did, however, accept US users. See SEC Charges Bitcoin-Funded Securities Dealer and CEO, SEC Litigation Release No. 24330 (November 1, 2018) available at **https://www.sec.gov/litigation/litreleases/2018/lr24330.htm**.
5. FinCEN requires persons or entities engaged in "money transmission services," defined as the acceptance of value substituting for currency from one person and the transmission of value substituting for currency to another location or person by any means, to register as MSBs and comply with the Bank Secrecy Act, AML and other regulations promulgated by FinCEN. Most US states also impose registration and other requirements on MSBs.
6. See Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001 (May 9, 2019); Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013).

their users are not identified on US sanctions lists as required by the Treasury Department's Office of Foreign Asset Control.[7]

While the US Treasury Department has yet to take public action against a DeFi company, FinCEN has previously shut down a non-US cryptocurrency trading platform for, among other things, failing to implement AML/KYC measures.[8]

Extraterritorial reach of US laws

As the Abra regulatory actions demonstrate, US regulators will assert broad jurisdiction against both US and non-US platforms and owners/developers for alleged violations of applicable US laws and regulations. The SEC, for example, may seek to assert jurisdiction over non-US persons for violations of the US securities laws based on conduct in the United States or effects on US markets. The SEC is likely to assert that US registration and other regulatory requirements apply to US and non-US developers whenever US persons can access or use a DApp or larger platform designed by the developer to offer or transact in securities. In the security token space, the SEC has brought enforcement actions against non-US entities that solicited or provided services to US persons through the Internet, as well as against individual software developers. While assertions of jurisdiction can and should be challenged in some cases, DeFi platforms should be mindful of US regulatory risks when designing their business and take steps to minimize their potential exposure.

The acting head of FinCEN, Kenneth Blanco, has made FinCEN's views on its jurisdiction clear, stating in May that FinCEN is "increasingly concerned that businesses located outside the United States continue to do business with U.S. persons without complying with our rules . . . [which require] registering, maintaining a risk-based AML program, and reporting suspicious activity, among other requirements."[9] To ensure that FinCEN's position was understood, he further emphasized that non-US virtual currency companies cannot "avail themselves of the U.S. financial system from abroad" without observing US AML requirements, and concluded that FinCEN is "serious about enforcing our regulations, including against foreign businesses operating in the United States as unregistered ["money services businesses" or] MSBs."

Impact on DeFi platforms

US and non-US platforms that provide US persons with services under the DeFi umbrella should proactively assess their US legal and regulatory exposure in the wake of Abra. It is clear from recent enforcement activity and public statements that US regulators like the SEC, CFTC, and FinCEN do not automatically consider software developers, smart contract creators, and other technologists to be outside their regulatory frameworks, even if they operate outside the US. Thus, DeFi firms should carefully review their protocols and measures taken to avoid US jurisdiction and validate their effectiveness, taking account of the lessons learned from Abra. If necessary, firms should consider terminating services to US users.

---

7. See, eg, OFAC Frequently Asked Questions, Questions on Digital Currency (March 2019) (stating that OFAC blocking requirements and transaction restrictions apply to technology companies, administrators, exchangers, and users of digital currencies) available at **https://home.treasury.gov/policy-issues/financial-sanctions/frequently-asked-questions/ofac-consolidated-frequently-asked-questions**.
8. *FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales,* FinCEN Press Release (July 26, 2017) available at **https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware**.
9. Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the Consensus Blockchain Conference (May 13, 2020) available at **https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-consensus-blockchain**.

CONTACTS

Steven Gatti
Partner
Washington
T: +1 202 912 5095
E: steven.gatti@cliffordchance.com

Megan Gordon
Partner
Washington
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

David Adams
Associate
Washington
T: +1 202 912 5067
E: davidg.adams@cliffordchance.com

Philip Angeloff
Counsel
Washington
T: +1 202 912 5111
E: philip.angeloff@cliffordchance.com

Jesse Overall
Associate
New York
T: +1 212 878 8289
E: jesse.overall@cliffordchance.com

Laura Nixon
Fintech Knowledge Lawyer
London
T: +44 20 7006 8385
E: laura.nixon@cliffordchance.com

Find more of our global fintech team at **www.cliffordchance.com/fintech**

For more information on Clifford Chance's global fintech capability and resources, or to be added to our weekly global fintech regulatory round-up, please email **fintech@cliffordchance.com**

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

2009-000298