

**C L I F F O R D**

**C H A N C E**



**FACEBOOK'S LIBRA –  
THE FINANCIAL  
CRIME RISKS**



**– THOUGHT LEADERSHIP**

OCTOBER 2019



## FACEBOOK'S LIBRA – THE FINANCIAL CRIME RISKS

Facebook's proposed global digital currency, Libra, aims to provide instant money transfers using blockchain technology for the 1.7 billion adults globally without access to a traditional bank account. Facebook says that Libra will be subject to regulatory oversight and review, but what will this regulation look like from a financial crime point of view, and will Libra be able to put in place suitable systems and controls that the unbanked can actually comply with? We consider the challenges for Libra in the face of the financial crime concerns that have been raised since its announcement.

The *White Paper*<sup>1</sup> that launched Libra in June states “*Libra’s mission is to enable a simple global currency and financial infrastructure that empowers billions of people.*” Leaving aside whether Libra is primarily intended as a financial inclusion tool (the founding members of the Libra Association, which will govern Libra, include businesses with many tech-sophisticated customers in developed countries), concerns have been raised about the potential for money laundering, tax evasion, hacking and terrorist financing.

### Policy maker reactions to date

Many world policy makers have reacted to Libra's announcement with scepticism and concern about the challenges Libra poses. For example, the French Minister of Finance, Bruno Le Maire, said: “I want to be absolutely clear: in these conditions, we cannot authorise the development of Libra on European soil.” Yves Mersch of the European Central Bank has also expressed concern, describing Libra as “beguiling but treacherous,” and his colleague Benoît Coeuré warned that “the bar for regulatory approval will be very high” for Libra to operate in the EU.

The US Government has also raised concerns that Libra, along with other cryptocurrencies, presents national security issues. Treasury Secretary Steven Mnuchin weighed in heavily at a press conference shortly after launch saying that Libra “could be misused by money launderers and terrorist

financiers,” that cryptocurrencies “have been exploited to support billions of dollars of illicit activity like cybercrime, tax evasion, extortion, ransomware, illegal drugs and human trafficking” and that he is “not comfortable” with the launch of Libra.

David Marcus, the head of Calibra, a Libra custodial wallet provider owned by Facebook, faced criticism at hearings before the US Senate Banking Committee and the US House Committee on Financial Services, with Congressman Brad Sherman stating “this is a godsend to drug dealers and sanctions evaders and tax evaders.”

The reaction in the UK has been more understated, with Mark Carney, Governor of the Bank of England, noting “The Bank of England approaches Libra with an open mind but not an open door. Unlike social media, for which standards and regulations are being debated well after they have been adopted by billions of users, the terms of engagement for innovations such as Libra must be adopted in advance of any launch.” It is interesting to note that Carney later suggested that a global digital currency similar to Libra “could dampen the domineering influence of the US dollar on global trade.”

The absence of traditional financial institutions in the Libra Association to date may indicate that financial institutions are wary of the potential financial crime risks, and are unwilling to become involved until there is more

<sup>1</sup> <https://libra.org/en-US/white-paper>

clarity on both Libra's proposals to address these risks and regulators' responses to these proposals. The Libra Association has only recently, three months post-launch, confirmed that it is pursuing a payment system licence from the Swiss Financial Market Supervisory Authority (FINMA) to tie in with its Swiss domicile in Geneva. It could also indicate that financial institutions may have commitments to other alternative payments projects or lack the technical infrastructure, know-how or personnel needed to meet Libra's initial membership requirements.

While there is a big difference between fiat currency and cryptocurrency (and blanket application of existing regulation of the former may not be suitable for the latter), financial crime threats exist for cryptocurrency as they do for traditional finance – and there are features of Libra which may exacerbate these threats.

## Crypto vulnerabilities

The UK Financial Conduct Authority (FCA) has warned of the rise of fraudulent online trading platforms for cryptocurrency. Reports of scams tripled in 2018 in the UK to over 1,800, with losses of over £27 million, of which 81 per cent of claims related to crypto scams.

A recent study by the University of Technology, Sydney found that 26 per cent of all Bitcoin users are involved in illegal activity, and, over the past two years, illegal use of Bitcoin has increased, despite the fact that parts of the online black market appear to be moving to cryptocurrencies offering greater anonymity such as Dash, Monero and ZCash.

Plainly, there is a risk that certain features of Libra could make it attractive to those engaged in illegal activity. The Libra protocol itself, which underpins the Libra Blockchain, does not link accounts to a real-world identity. Libra takes a similar approach to Ethereum and Bitcoin in providing pseudonymity – a state of disguised identity in which the account holder is identified according to a unique alphanumeric string (public address), but not by their real identity. Only the sender's and receiver's public addresses, the transaction amount, and the timestamp

are publicly visible on the Libra Blockchain for each transaction.

Financial institutions are required, under anti-money laundering (AML), counter financing of terrorism (CFT), sanctions and similar laws and regulations in many jurisdictions globally, to take steps to identify customers, verify their identity and understand the purpose and nature of financial transactions and relationship with the institution. Additional checks, such as obtaining information on the source of funds and on the source of the underlying owners' wealth, may be required if a customer is a politically exposed person (PEP) or otherwise classified as high risk.

Instead of conducting these checks and diligence on the parties to each Libra transaction (as a financial institution would generally have the responsibility to do), the Libra Association may seek to rely on others to do so, although the details remain unclear.

The Libra Association appears to take the view that it is a governing body or membership consortium overseeing a software network – not a financial institution that interfaces with consumers or end users – and that responsibility for transaction-level diligence should therefore lie with the intermediaries that do interface directly with consumers and end users and provide them with the “on and off ramps” necessary to access the Libra network and engage in Libra transactions (e.g., wallet providers, exchanges, etc.).

A letter from David Marcus to the US Senate Banking Committee dated 8 July 2019 explains that “The Libra Association itself will not be involved in processing user transactions and will not store any personal data of Libra users.” This “personal data” would presumably include information on a person's real-world identity. Without such data, it is unclear whether and how the Libra Association could actively screen Libra users for AML, sanctions, or other purposes. Instead, the letter states that: “Third party developers will be able to build on top of the Libra Blockchain, including by building digital wallets. It will be the responsibility of these [wallet] providers to determine the type of information they may require from



their customers and to comply with regulations and standards in the countries in which they operate. Regulators of Calibra and other digital wallet services can require them to collect information about the identity and activities of their users and make such information available to law enforcement and regulatory agencies, such as for AML, CFT, and sanctions purposes.”

An exchange in the US Senate Banking Committee hearing on Libra between Senator Catherine Cortez Masto and David Marcus on 16 July 2019 regarding AML compliance responsibilities on the Libra network further supports this interpretation:

**Senator Cortez Masto:** “Would the [Libra] Association itself fall under the Bank Secrecy Act jurisdiction?”

**David Marcus:** “Senator, the Association will not actually touch consumers...”

**Senator Cortez Masto:** “So who’s going to be subject to the Bank Secrecy Act and [the jurisdiction of the U.S. Treasury Financial Crimes Enforcement Network, or] FinCEN then?”

**David Marcus:** “So the Calibra wallet, and all of the wallets that are operating under their jurisdiction, will of course comply with the Bank Secrecy Act, will perform KYC and have AML programs...”

Marcus maintained a similar line of argument regarding responsibility for sanctions compliance, saying that sanctions compliance would be conducted by service providers (e.g., wallet providers and exchanges) and not by the Libra Association:

**Senator Cortez Masto:** “The head of policy and communications for Libra was recently on a podcast and was asked how Libra would react if a government like the United States required that the Libra Association blacklist certain addresses in order to comply with sanctions laws. The response was, I quote, ‘The Association won’t interact with any jurisdiction, it will instead leave that to the entities that provide an on-and off-ramp to the Libra currency.’ Can you clarify that? How are we supposed to address this

issue when it comes to blacklisting and sanctions laws?”

**David Marcus:** “... I believe [the basis for the comments] may be because the Association itself is not running anything, it’s just coordinating governance, but the actual service providers that are going to be regulated service providers will enforce [the funds’] travel rule, perform [Office of Foreign Assets Control, or] OFAC checks, and ensure that those who are subject [to regulation] will, of course perform those functions.”

While this exchange pre-dates the Libra Association’s recent confirmation of its intent to apply for a payment system licence from FINMA which may indicate a shift away from this view, there is still no clarity. This raises several broad sets of challenges.

## Interaction with traditional finance

We have already noted that no banks have been announced as Founding Members of the Libra Association, and that wanting more clarity on the regulatory status and the controls to manage financial crime risk associated with Libra may be a factor in the decision of those institutions not to participate so far.

In order for proceeds of crime to enter and be laundered through the finance system, there must first be placement of those proceeds within it. Some in the crypto industry have argued that banks and other regulated financial institutions have a ‘gatekeeper’ role – in which they are the ones that apply the necessary financial crime diligence, which provides assurance that proceeds of crime will not make their way into the traditional finance system. This ignores, however, the financial crime risks associated with anonymous transfers within the system, and in the current climate, where significant penalties from regulators for money laundering breaches by financial institutions are a regular occurrence, and regulatory focus remains on financial crime, there is little incentive for financial institutions to risk interfacing with the boundaries where cryptoassets and fiat

current meet (e.g. by providing custodial services or handling money derived from them). Banks are unlikely to be open to taking funds that have been exchanged out of pseudonymous cryptoassets.

This is likely to change over time. If Libra ‘takes off’ in the way it is proposed and operates as a standard marketplace tool, not just for the unbanked, but also for consumers more generally, then there will be increased pressure for banks to interact with cryptoassets. Aside from Libra, many banks are involved in other crypto initiatives like the Utility Settlement Coin and JPM Coin. We have also seen signs that central banks are increasingly open to issuing their own cryptocurrencies. With an increased scale of activity comes increased risk, and without robust financial crime controls within the crypto industry, the risk of financial crime facilitation greatly increases.

What is clear that, in circumstances where scrutiny is required only at the touchpoints, then this heightens the risk. As with any virtual currency, if the only people carrying out KYC and monitoring are the goalkeepers at either end (specifically the wallet providers and exchanges which Libra appears to intend to rely on) then anything could happen in the middle where the pseudonymous nature of Libra means transparency is limited.

## **Regulator attention**

Cryptocurrencies are under increasing scrutiny from regulators and policy makers – and Libra will be no different. The Financial Action Task Force (FATF) Recommendation 15, adopted in June this year, means that cryptoexchanges and other “virtual asset service providers” will be subject to regulation and supervision/monitoring with respect to AML in FATF member countries. This includes having to share originator and beneficiary information during transactions between exchanges under the ‘travel rule’ – an onerous requirement for systems built on pseudonymity and one which, it has been warned, may drive cryptocurrency transactions off platforms which give some visibility over

financial crime. The FATF’s recommendations – while described as “recommendations,” are unlikely to be ignored in most jurisdictions.

The implementation of the EU’s Fifth Money Laundering Directive (5MLD) will also take effect in January 2020 and introduce regulation for crypto-to-fiat exchanges and custodian wallet providers, who must now be registered with the competent authority where they are domiciled. It is expected that, particularly in light of FATF Recommendation 15, jurisdictions such as the UK will “gold plate” their implementation of the Directive into national law, so that regulation is likely to be applied to all digital assets and not just cryptocurrencies, to exchanges more broadly (and not just crypto-to-fiat) and extra-territorially to those providing services to people in the relevant jurisdiction, even where the provider is based outside.

As outlined above, the Libra Association was established in Geneva and it has recently announced its intention to apply for a payment system licence under FINMA, following the Association’s submission of a request for ruling to clarify its regulatory status. Calibra is registered in the US with the Financial Crimes Enforcement Network (FinCEN) as a money services business (MSB). Thus, Calibra will be subject to certain MSB requirements including maintenance of an adequate AML compliance program, where it carries out activities bringing such requirements. Marcus told the US Senate Banking Committee that the Libra Association also intends to register with FinCEN, though he did not discuss the anticipated scope of its AML responsibilities or clarify how the Association might meet any such responsibilities with regards to end users.

The Libra Association’s proposal to push down responsibility for transaction-level AML, KYC, CFT and sanctions compliance to service providers, such as wallets and exchanges, will continue to attract regulatory scrutiny until there is more clarity. This concern is likely to be heightened by the White Paper’s

announced ambition to eventually make the Libra Blockchain permission-less and open-access to all. If responsibility for transaction-level compliance ultimately rests with wallets, exchanges, and other service providers around the world and not with the Libra Association that controls and administers the overall technology platform (and is arguably the penultimate “gatekeeper”), regulators will almost certainly worry about unscrupulous service providers attempting to use Libra to launder money, circumvent sanctions and engage in other illegal activity, particularly where the eventual permission-less environment will allow them to control their own access to the platform.

Wallets and exchanges, the entry and exit points into and from the Libra system, could, for example, seek some regulatory arbitrage in establishing themselves in jurisdictions with lower standards of financial crime law and regulation. This could allow suspect funds to enter the Libra system in a more lax jurisdiction and exit it somewhere with higher standards – and without sufficient transparency in between due to the pseudonymous nature of Libra. There is a risk that the strength of the Libra system will therefore be measured by the weakest endpoint, to be found in the location with the lowest financial crime standards and enforcement.

### The target audience

The White Paper states that Libra is targeted at the unbanked, and further states that it is essential to the spirit of Libra that the Libra Blockchain will be open to everyone. It says: “Open access ensures low barriers to entry and innovation and encourages healthy competition that benefits consumers. This is foundational to the goal of building more inclusive financial options for the world.”

The difficulty with this target audience is that, often, they lack the basic items which are taken for granted when opening a bank account – birth certificates, passports, utility bills. Fintechs have been creating products for the unbanked in recent years, with challenger banks such as Monzo in the UK offering the ability to make online payments to those with limited financial inclusion. However, Monzo is still a bank, regulated in the UK by the

FCA, and subject to its jurisdiction. Multiple members of the Libra Association are US payment processors subject to US AML and sanctions requirements. It is difficult to see how such organisations will be able to provide services to unbanked customers without access to birth certificate, passport, or similar information.

### What’s next?

The Libra Association has stated that it will “work with the community to gather feedback on the Libra Blockchain prototype and bring it to a production-ready state”. A report being produced for G7 finance ministers in October, may bring further clarity. However, so far there is uncertainty about the action that the Libra Association is taking to get regulators and government agencies on board. David Marcus of Calibra has stressed that Libra will not be offered until it has “fully addressed” regulators’ concerns and received approval. However, Marcus’ testimony to this effect in front of the Senate Banking and US House Committee on Financial Services has not put an end to politicians calling for the launch to be halted entirely until the Libra Association has obtained all approvals. The Libra Association has recently said that post-launch it has maintained its commitment that “technology-powered financial services innovation and strong regulatory compliance and oversight are not in competition” and that it is “engaging in constructive dialogue with FINMA” with “a feasible pathway for an open-source blockchain network to become a regulated, low-friction, high-security payment system.”

Establishing the necessary network of financial institutions, and obtaining the approvals required to move fiat currency around the world, each take time and effort. Firms are required under anti-money laundering legislation (which exists in some form in all sophisticated jurisdictions, and in many less sophisticated jurisdictions too) to have complex systems and controls in place to minimise financial crime risks. Without taking meaningful steps to address the concerns that have been raised since the launch of Libra, the Association may struggle to make the target launch date of the first half of 2020.

## AUTHORS



**Ellen Lake**  
Senior Associate  
London  
T: +44 20 7006 8345  
E: ellen.lake@cliffordchance.com



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



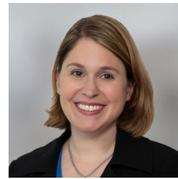
**David Adams**  
Associate  
Washington  
T: +1 202 912 5067  
E: davidg.adams@cliffordchance.com



**Peter Chapman**  
Partner  
London  
T: +44 20 7006 1896  
E: peter.chapman@cliffordchance.com



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



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



**Michael Lyons**  
Partner  
London  
T: +44 20 7006 4317  
E: michael.lyons@cliffordchance.com



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



**Lena Ng**  
Partner  
Singapore  
T: +65 6410 2215  
E: lena.ng@cliffordchance.com



**Andrea Tuninetti Ferrari**  
Senior Associate  
Milan  
T: ++39 02 8063 4435  
E: andrea.tuninettiferrari@cliffordchance.com



**Arun Visweswaran**  
Senior Associate  
Dubai  
T: +971 4503 2748  
E: arun.visweswaran@cliffordchance.com



**Donna Wacker**  
Partner  
Hong Kong  
T: +852 2826 3478  
E: donna.wacker@cliffordchance.com

## CONTACTS

C L I F F O R D

C H A N C E

This publication does not necessarily deal with every important topic nor cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

[www.cliffordchance.com](http://www.cliffordchance.com)

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

© Clifford Chance 2019

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](mailto:nomorecontact@cliffordchance.com) or contact our database administrator 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.