August 1, 2022

FinClusive Capital, Inc.
860 Bullock Drive Guilford, VT 05301
contact@finclusive.com

California Department of Financial Protection and Innovation
Legal Division
Email: regulations@dfpi.ca.gov

Re: Invitation for Comments – Crypto Asset-Related Financial Products and Services

Dear Sir/Madam,

As a company dedicated to bringing compliance-centered equitable financial services to the financially excluded or underserved, we appreciate the opportunity to provide input to the State of California's Department of Financial Protection and Innovation (DFPI) in regards to Governor Gavin Newsom's Executive Order (N-9-22) aiming to create a transparent regulatory and business environment for web3 companies that will harmonize both federal and state approaches, balance the benefits and risks to consumers, and incorporate California values such as equity, inclusivity, and environmental protection.

Company Background

FinClusive is a hybrid regulatory technology (Regtech) and financial technology (Fintech) company dedicated to bringing compliance-centered financial access to the 2.5 to 3.5 billion people and millions of businesses worldwide who are financially excluded or underserved. FinClusive delivers on this mission by (i) providing a comprehensive and modernized full-stack financial crimes compliance (FCC) solution for bank and nonbank financial intermediaries (including decentralized financial services (Defi), blockchain enabled, and virtual asset services providers (VASPs), and (ii) facilitating access and the secure movement of funds through traditional (ACH, Wire) and blockchain enabled payment rails. These dual and complementary services enable FinClusive to provide comprehensive compliance services that are a 'gateway' to secured accounts and payments capabilities via FinClusive's growing U.S.-based bank of record (BoR) partners. FinClusive is registered with FinCEN as a nonbank Money Services Business (MSB) and is in the process of obtaining money transmission licenses across all applicable and necessary US states and territories. FinClusive's capabilities enable a larger universe of organizations to engage in the provisioning of financial services to underserved, excluded organizations, or those otherwise considered "higher perceived compliance risk."

Leading Industry Standard Best Practices – Compliance and Inclusive Finance Working Group

FinClusive leads a sector-based working group—the Compliance and Inclusive Finance Working Group (CIFWG), which is comprised of a global consortium of traditional and alternative financial services providers dedicated to the modernization of FCC controls that comports with industry innovation and is devoted to financial inclusion. The purpose of the CIFWG and its members is to advance the mission of financial inclusion globally by addressing the challenges and opportunities presented by innovations in the financial services and payments landscape, and the attendant financial and regulatory compliance implications. CIFWG is an open group of traditional bank and non-bank financial institutions, regulators, policymakers, technologists, ethicists, and legal experts which monitors the challenges faced by the financially excluded and underserved and focuses on how economic and regulatory technologies can bridge the gap between traditional banking compliance and associated risks injected by innovation.

In this endeavor, the CIFWG has developed and promotes the *Rulebook*, an innovative best practices framework that extends traditional banking compliance and payments guidance to emerging fintech and VASP processes. The *Rulebook* works proactively with the growing fintech sector—including and especially organizations engaged in crypto and virtual asset-related services—to ensure essential global financial regulatory compliance while accommodating nonbank financial service providers' and fintechs' seamless experience and smooth flow of funds for members and reinforcing the application and intersection with traditional banking rails. By design, the *Rulebook* is open source and dynamic in nature to ensure it reflects ongoing proposed rules and best practices related to AML/FCC compliance as applicable to the growing alternative financial services and virtual asset sector and motivated toward a more inclusive financial services economy, a modernized financial market infrastructure that 'embeds' essential AML/FCC controls within its operations and technology infrastructure, and applicable to the activities and practices undertaken by institutions engaged in 'covered' financial services activities.

The *Rulebook* defines technical standards for end-to-end transaction flows and service-level agreements between parties to reflect the operational realities of an increasingly decentralized and cross-border financial system. Driven by the industry and informed by global regulators and policy makers, the *Rulebook* is a dynamic framework that reflects the operational realities of these growing payment technologies and builds upon existing governance and data privacy rules from the following organizations:

- Financial Action Task Force (FATF)
- Society for Worldwide Interbank Financial Telecommunication (SWIFT)
- National Automated Clearing House Association (NACHA)
- National Institute of Standards and Technology (NIST)
- European Union's General Data Protection Regulation (GDPR)
- Bank for International Settlements' (BIS) Committee on Payments and Market Infrastructures (CPMI)
- Digital and Self-Sovereign Identity (SSI) Principles as Advanced by the Sovrin Foundation

In advancing its mission, CIFWG engages with and through other international organizations, initiatives, and regulatory-led groups that advance financial inclusion and modern regulatory compliance solutions. CIFWG recognizes and incorporates important innovations in Its ultimate goal to promote access to traditional and non-traditional financial services and highlight the resulting benefits of building economic resilience and prosperity that directly relate and contribute to our national and international security.

Overview and Framing of the Invitation for Comments

FinClusive appreciates DFPI's commitment to bringing transparency and regulatory clarity to the growing virtual asset sector to address potential areas of governance and risks associated with illicit finance and is encouraged that DFPI is continuing to foster trust with members of industry by seeking consultation and comments. For too long, outdated and unduly onerous regulations have hindered innovation and growth in digital asset and blockchain technology markets, and inconsistency across jurisdictions has made compliance with requirements challenging and, in some cases, impossible. By engaging with new technologies to automate certain processes and harmonizing California requirements with those of the federal government and other global standard-setting and regulatory bodies, DFPI can create a newly fertile environment for collaboration with digital asset providers.

Some of our concerns revolve around the overly broad application of registration obligations to facilitators of (or more specifically, those identified as being "involved with") VASP-related activities (such as Defi protocols or applications), that would be challenging and costly, but also threaten to stifle innovation and potentially drive growth and use of virtual assets to unregulated and non-transparent channels. Other concerns relate to the potential unintended consequences to promoting and supporting financial inclusion—a central objective

to creating a safe and secure financial system for all—where ongoing innovation in the virtual asset services sector has great potential in enabling access for marginalized, underserved and excluded communities.

Our letter focuses on the importance of financial inclusion as a central element of the virtual asset sector, and recommends a modernized approach to regulations that better reflect:

1. the new and different operational and technology realities underpinning virtual asset activities (e.g. blockchain/distributed ledger technology (DLT), peer-to-peer or non-intermediary-based financial services, borderless interconnectedness, the growth in digital inclusion worldwide) that are vastly different from traditional financial services operations and technological architecture and their attendant regulatory compliance requirements,
2. the coverage of and application of essential AML/FCC controls that are aimed to the "activities and practices" undertaken by both traditional and nontraditional financial services providers (of all types), and
3. the importance of the risk-based approach in addressing regulatory risks related to particular actors in the financial services ecosystem, ensuring that the application of regulatory controls fall on those actors undertaking 'activities and practices' that warrant such coverage.

Financial Inclusion Needs to Be Included as an Explicit Measure of Effectiveness

As the invitation for comments affirms, financial inclusion remains a desirable and necessary goal for California. As a state with a diverse and growing population, including immigrants who may want to remit money to their families in their home countries and small to large legal entities with global reach and therefore financial services needs, California's consumers are affected by the many areas of the world having limited on no access to traditional financial services (see Figure 1). While financial services access is often viewed as an issue for emerging or frontier markets and/or those jurisdictions with higher rates of low/moderate income, financial exclusion continues to be a reality globally including with and for more developed markets, such as the United States. Despite minor improvements in recent years—particularly with respect to providing basic account access to the fully unbanked—the number of unbanked and underbanked remains high,[1] which further undermines our collective efforts to enable underserved and marginalized communities to build sustainable financial health patterns that deliver economic resilience. Within California, the foreign-born population is approximately 26.6% of the total population[2] and estimates indicate that approximately 5% of households in the U.S. report sending monetary transfers to relatives and friends outside the U.S.[3], suggesting that at least 655,000 households in California are involved in these monetary transfers.

Importantly, "de-risking"—the efforts of financial institutions to terminate or restrict relationships of certain clients and customers—has continued to be amplified by the continued growth of global anti-money laundering/counter-financing of terrorism (AML/CFT) controls.[4] The result is a disproportionate impact for the financially underserved, the global poor, and institutions and sectors that provide services to these segments of the economy, including but not limited to: international correspondent banks, nonprofit/humanitarian organizations and international remittance companies or money services businesses/money transfer operators (MSBs/MTOs).[5]

[1] Federal Deposit Insurance Corporation. (2020, October). *How America Banks: Household Use of Banking and Financial Services, 2019 FDIC Survey*. https://economicinclusion.gov/downloads/2019_FDIC_Unbanked_HH_Survey_ExecSumm.pdf
[2] U.S. Census Bureau. *2020 American Community Survey*. https://data.census.gov
[3] U.S. Census Bureau. (2020, November). *Who in the United States Sends and Receives Remittances? An Initial Analysis of the Monetary Transfer Data from the Aug. 2008 CPS Migration Supplement*. https://www.census.gov/library/working-papers/2010/demo/POP-twps0087.html
[4] https://www.worldbank.org/en/topic/financialsector/brief/de-risking-in-the-financial-sector
[5] https://www.worldbank.org/en/topic/financialsector/publication/world-bank-group-surveys-probe-derisking-practices

Figure 1. Global Unbanked Adults, 2017[6]

Many MSBs/MTOs have seen banking services denied, downgraded, or made more expensive, and many are pushed out of one bank and are forced to find another that may be more costly, requires multiple intermediaries through which to send payments, or otherwise pursues less transparent or informal or unregulated channels for the transfer of value. The Center for Global Development and other think tanks and industry groups have shown that many smaller MSBs/MTOs have been forced to close, become agents of larger businesses, or even disguise the true nature of their operations in order to remain banked.

In fact, the virtual asset sector—and companies deploying blockchain and distributed ledger technologies in the context of cross border remittances and payments—have themselves continued to be the victims of de-risking by banks when seeking institutional bank accounts or bank partnerships that could enable their customers into formal accounts. Despite guidance by U.S. and global regulators that such activities should be evaluated on a case-by-case basis, wholesale denial of services to the sector continues in certain jurisdictions where the risks to reputation or the cost-benefit of taking on such business given the hazards of regulatory sanction or large fines compel formally regulated financial institutions to stay away from these business activities entirely.[7] Importantly, as VASPs and blockchain-enabled businesses continue to propagate in the market providing potential solutions to bring more financially marginalized communities into financial services, their categorization by many states and the federal government as money service businesses (MSBs) puts them under further scrutiny as a potentially 'high perceived compliance-risk' businesses – as evaluated by both regulators (state and federal) and banks whose services they rely upon for both operational and customer-related activities.

[6] Global Findex Database: https://globalfindex.worldbank.org/sites/globalfindex/files/chapters/2017%20Findex%20full%20report_chapter2.pdf
[7] https://www.forbes.com/sites/pawelkuskowski/2020/02/20/europes-new-aml-directive-means-banks-can-no-longer-shut-crypto-out/?sh=24f217f05466

In 2017, the G-20 committed to advance financial inclusion worldwide and support the G-20 Global Partnership for Financial Inclusion (GPFI). The G-20 High Level Policy Guidelines on Digital Financial Inclusion for Youth, Women and SMEs published in 2020 stated that the COVID-19 outbreak has amplified the critical need for digital access to affordable financial products for individuals to ensure continuity of access to financial services and sustaining remittance flows. Alternative financial services providers including VASPs, nonbank FIs and decentralized financial services applications have continued to innovate (in particular related to the ease and efficiency of accessing accounts—including digital wallets—and in transmitting value and making payments) to serve these market segments, provide essential efficiencies for financial access in an increasingly digitizing economy with increased opportunities through web/application-based services, and reach populations underserved by traditional financial services providers.

While individual banks may be acting *rationally* by refusing to service certain types of organizations or those conducting certain activities or operating in particular jurisdictions, the continued growth in AML/FCC has created client categorizations of higher perceived risk such that these institutions are unable to justify the associated compliance costs. This nature of financial exclusion—specifically due to ***de-risking***—creates further challenges to address equitable financial access and economic opportunity, and therefore national security, especially when impacting cross-border funds flows that are the lifeblood for many individuals, households, small businesses and whole economies.[8] Sustainably addressing financial inclusion pays dividends to our broader economic and national security interests.

There are a number of reasons why certain individuals and organizations are (or remain) underserved or excluded from the formal financial services sector. Digitization and innovation have continued to address some, but not all of the current challenges. Issues related to minimum account balances, high/unpredictable fees, concerns about privacy and lack of trust in traditional financial institutions and the operational realities (branch locations and hours) are alleviated or minimized through these methods. These new applications enable consumers and businesses to engage in needed services while keeping them in control of their funds and transactions in ways that traditional intermediary-based banking services have denied them. However, their continued labeling as 'high risk' continues to stifle meaningful engagement between traditional financial services participants and rapidly growing alternatives like VASPs and other fintech and blockchain-enabling activities.

As such, we must work to mitigate measures that put undue additional burdens on such technology-enabled non-traditional financial services and the stigma that has been unfairly placed on blockchain-enabled financial services and the (mis)perceived risks regarding the use of such technology applications as they serve to undermine overall effectiveness in driving financially-inclusive remedies that can bring more individuals and organizations into the regulated financial services system and ultimately improve their financial resilience and economic security. For example, as regards to the growth of self-hosted wallets to bolster global financial inclusion, their growth via these technology applications can serve to enhance security while bringing down costs--these transactions could significantly revolutionize global remittances, where just a 5% reduction in cost of global remittance would boost payments by $16bn.[9]

Further, in certain instances, such as the conflict in Ukraine or addressing needs in humanitarian and high-conflict zones, these applications are proving to be the only mechanism in which individuals are accessing economic resources. As an example, in Ukraine, the ability for the government to raise millions of dollars of support through virtual assets, and individuals and merchants being able to download digital asset wallets to transact in a peer-to-peer manner becomes essential to their economic survival and reinforces more tools in

[8] https://www.worldbank.org/en/topic/migrationremittancesdiasporaissues/brief/migration-remittances-data
[9] https://theblockchainassociation.org/wp-content/uploads/2020/11/Self-Hosted-Wallets-and-the-Future-of-Free-Societies.pdf, P42

the US national security toolkit. Building economic resilience should be central to our goals of strong, globally sustainable FCC requirements.

Consider a New Framework Based on Activities and Practices

Regulatory innovation lags behind commercial financial sector innovation. Traditionally, rules governing AML/CFT protections and FCC obligations have been considered in the context of the nature and form of financial market participants, and as such have been amended or enhanced by regulators looking to address specific operational nuances of such actors. These have largely been against entity type (e.g. bank and nonbank financial institutions (NBFIs), designated non-financial businesses and professions (DNFBPs), and are being extended to the rapidly growing fintech sector and the growth of alternative financial services ecosystems including those on blockchain protocols and decentralized networks. In addition, regulations governing money transmission licensing have failed to keep pace with the rapid growth of technology solutions and are currently tailored primarily to fiat currency-based traditional money transmitters without taking into account the significant differences in fiat and virtual asset issuance and payment activities in a peer to peer and decentralized or non-intermediary based ecosystem.

Current guidance establishes intentionally "expansive" definitions of VA and VASPs that extend far beyond traditional notions of regulated financial activity into non-financial activity and businesses of and by related or third-party participants.,[10] and this expansive view goes beyond what is traditionally regulated as a non-bank money services business (which is the current default regulatory framework covering VASPs in many countries, such as the United States).[11] As a result, numerous entities whose activities would ordinarily not be treated as regulated money services businesses are in fact treated as such, and thereby inappropriately subject to the FATF's customer due diligence and travel rule requirements. This approach renders an overly expansive regulatory framework that will have implications for such businesses, many of whom operate across multiple jurisdictions and diverse regulatory regimes. It is important to note that the manner in which MSBs/MTOs are governed in the U.S. requires such companies to ensure licensing and regulatory compliance both at the federal level as well as all individual states, many with differing regulatory and supervisory standards governing their activities in their particular states. Such realities have very real costs to these businesses whose uncertain and differing US regulatory obligations have serious competitiveness consequences for U.S.-based operators.

Given the varied nature of virtual asset activities in particular, the application of regulatory licensing and essential FCC regulations should instead be determined by a sector participant's *activities and practices* to avoid overly broad definitions that could stifle innovation or misapplication of necessary FCC obligations to relevant parties in keeping with a risk-based approach. In order to reap the benefits of virtual asset and fintechs' ability to reach the financially excluded, and better align intended controls to the changing operational and technological realities of this fast-growing sector, we believe a reframing of regulations and consumer protections is necessary in order to better serve consumers where alternative financial services providers can provide a more efficient and lower-cost alternative to the traditional banking system that has to date excluded many of those same consumers.

Activities and Practices

[10] See Guidanceat ¶ 41 ("[t]he definition of VA is meant to be interpreted broadly"); ¶ 48 ("the definition of VASP should be read broadly"); ¶ 60 (the safekeeping and administration limbs of VASP definition "should also be read expansively").

[11] US Treasury's FinCEN regulates those money services businesses (the presumed equivalent of a VASP) typically on the basis of providing money transmission services, which is defined as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds or other value that substitutes for currency to another location or person by any means." 31 CFR § 1010.100(ff)(5) Individual U.S. states such as California further regulate these business through licensing regimes or other methodologies.

Ongoing modernization of FCC applications has lagged behind the industry and the current level of innovation in the commercial financial sector, which has brought new entrants—both from within financial services and outside of it engaging in the provision of financial products and services that equally require an updated governance approach. Traditional AML/FCC controls have been challenging for traditional financial services participants; the building of tokenized financial services underpinned by blockchain and DLT requires a re-thinking on how we approach regulatory compliance requirements that 1) take advantage of the technology attributes that ***actually serve to protect and enhance transparency*** of customers and their transaction activities, while enabling faster, cheaper and more efficient ways to access and engage financial services and products. A new approach focused on these *activities and practices* could bring significant and forward-looking advantages to include:

- Acknowledgement of continued evolution and innovation in financial services—and in particular in the virtual asset services domain built on DLT and new applications built natively on the web—occurring outside the traditional financial sector, and drive greater inclusion opportunities,
- Better represent the operational realities that vary considerably from traditional bank/nonbank and fiat-based financial intermediary activities, particularly those related to the issuance, storage/custody, and transfer of value,
- Extend FCC legal and supervisory regimes that better comport with ongoing innovation in the financial sector broadly, including leveraging the attributes of blockchain to enhance oversight and supervision,
- Incentivizes existing and new financial services entities to self-govern for the good of all participants, clients and counterparties for or on whose behalf they are facilitating or enabling such services—establishing and reinforcing safe/secure access, consumer protection and privacy, and protections against exploitation by illicit actors, and
- Reinforces the joint goals of financial inclusion and global financial system integrity, which to date have continued to be seen by the sector as a false binary choice.

The CIFWG's best practices *Rulebook* is specifically aimed at governing by *'activities and practices'*, as undertaken by these diverse financial market participants, as opposed to governing based on entity type or siloed regulatory supervision. By building a framework focused on the "constants" in the financial system, the *Rulebook* endeavors to create an effective yet nimble approach to governance in a highly innovative and ever-changing environment.

The framework defines the operational rules and procedures for network participants, who:

- create or issue digital units/stores of value;
- are custodians of (storing) digital units/stores of value;
- transact (sending or receiving) digital units/stores of value (i.e. transactions); or
- provide liquidity with/between one or more network participants, which include transfers:
    - within the network itself,
    - between traditional banking rails and a particular digital payments network.

Leveraging Technology Underpinning Virtual Assets to Facilitate Greater Inclusion

As virtual asset services continue to evolve and grow, so do the applications and opportunities inherent in facilitating greater inclusion of underserved and marginalized communities and organizations into a continually evolving global financial ecosystem.

DLT has emerged as an additional potential value additive capability that has applications to both driving secure, cost-efficient value transfer as well as enhanced compliance to meet AML/CFT goals and obligations. DLT is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple

sites, countries, or institutions, and blockchain technology—a form of DLT—has characteristics that can facilitate stronger compliance and inclusion in tandem:

- *Distributed*: Blockchain creates a shared system of record among business network members—eliminating the need to reconcile disparate ledgers.
    - Transactions via blockchain networks can be constructed and held throughout the network and ultimately accessible via secured channels for audit and tracking purposes. This can be very helpful with respect to both client and transaction-related data, and the protection and presentment of KYC (identity) data between corresponding financial intermediaries.
- *Immutable*: Consensus is required from all members and all validated transactions are permanently recorded. Even a system administrator cannot delete or alter a transaction.
    - Transactions can be recorded for auditability and transaction monitoring for AML and anti-fraud purposes. The near-real-time settlement functionality can facilitate close to real-time payments between counterparties as opposed to 3-5-day settlement times via traditional channels. Transaction history and specifics cannot be altered once recorded, which means the associated identities of senders and receivers of a transaction can be verified as associated with the transaction itself. The immutability of the ledger can therefore benefit ongoing client and transaction monitoring real time—increasing process efficiencies and reducing costs associated with compliance activities.
- *Permissioned*: Each member of the network must have access privileges and information is shared only on a need-to-know basis between network nodes.
    - Information regarding the transaction origin (sender) and recipient can be permissioned between nodes for easy and secure access without disclosure to third parties without permission, and be leveraged for verification/validation purposes, managing against fraud, and assisting network participants in a common financial ecosystem.

While the applications for blockchain and other technologies are far reaching, one can easily see where they can add value specifically to underserved/excluded markets as well as in the furtherance of AML/CFT goals, such as those ***related to KYC and CDD*** and the ***use and verification of financial market participants' identities***. Modernized identity verification and management is central to the KYC/KYB process and is the common currency in ensuring FCC elements enable inclusion of legitimate actors and the exclusion of illicit actors. The use of a Decentralized Identifier (DID) alongside a KYC/KYB compliance-backed verified credential can provide a stronger value proposition for identity verification and trust networks, and responsible and disciplined application testing and deployment of such technology alongside regulatory oversight will pay dividends to the industry, regulators and law enforcement alike.

Further, currently centralized exchanges and other VASPs are already obligated to have in place appropriate FCC controls, and the information collected to drive KYC/KYB, due diligence, monitoring, and analytics have continued to evolve and be applied by sector participants. In addition to the technology attributes described above as serving to aid law enforcement and regulatory oversight, additional blockchain analytics tools continue to evolve with significant benefit to law enforcement. Today, law enforcement authorities—with sufficient legal basis—can request and obtain information from covered entities (including VASPs) regarding transactions and customer history and profiles. This information, coupled with the ***immutability and pseudonymity*** of transactions in most blockchains—along with KYC/KYB data related to such customers and clients—is already proving useful to law enforcement. Expanding the scope of regulatory compliance to 'facilitators' or others merely 'involved with' such activities will serve to cool such innovation or drive their activities away from regulated jurisdictions and/or channels that already benefit from such oversight.

<u>Consequences to Inclusion-Oriented Technology Applications: e.g. Self-Hosted Wallets</u>

Self-hosted wallets are playing an increasingly important role with virtual assets, as global financial operations continue to be unbundled (individual products and services are increasingly provided by financial market players, including nonbank financial institutions/financial technology companies and outside formally regulated traditional bank FIs) and an ongoing trend toward de-centralized financial services continues unabated. Despite this growth, assumptions continue to be made as to the *inherently* suspicious nature of self-hosted wallets, despite data to the contrary. As part of its ongoing review and monitoring of the sector, the Financial Action Task Force (the inter-governmental body setting international standards regarding global money laundering and terrorist financing) has also commented that self-hosted wallets posed a limited risk for money laundering and terrorist financing[12].

Self-hosted wallets enable anyone with an internet connection to transact with others in digital assets on a peer-to-peer (P2P) basis. Additionally, these wallets can be used to store value or digital assets securely and provide capability for the user/consumer to hold resources personally that enable them to interact in the fiat and digital financial context. The items in a personal wallet, such as cash, credit and debit cards, driver's licenses and other forms of identification enable such access and facilitation of transfers of value connected to institutions custodying or transferring such value. This enables that consumer to transact with counterparties directly without the need for a third-party intermediary–similar to making a cash transaction for a purchase of a good, paying an expense, or transferring value to a friend or family member—but in this case with enhanced traceability afforded through DLT including to immediately verify identity.

Similarly, self-hosted wallets, including those created by open-source software connected to alternative financial ecosystems in the virtual asset sector perform the same function—enabling the handling and use of personal identity and financial assets/tools directly. This enablement can serve to break down barriers to financial access including and especially for marginalized communities (individuals and organizations) that have otherwise struggled to obtain or maintain access to formal financial services. As cash-based transactions continue to trend lower and digital connectivity continues to trend higher globally, self-hosted wallets represent opportunities for inclusion[13] that provide both the ease of digitally-based interactions and the security and traceability protocols that do not exist with fiat cash-based transactions. Indeed, the growth in P2P applications correlates with the drive toward more comprehensive digital inclusion and is reflected in the growth in technology adoption more broadly, including and especially mobile and smartphone penetration rates and the interconnectivity of electronic value transfer. Innovation in this space, leveraging self-hosted or noncustodial wallets, is also enabling further innovation in the virtual asset ecosystem, including central bank digital currencies (CBDCs), peer-to-peer payments, and cross-border remittances to name just a few.

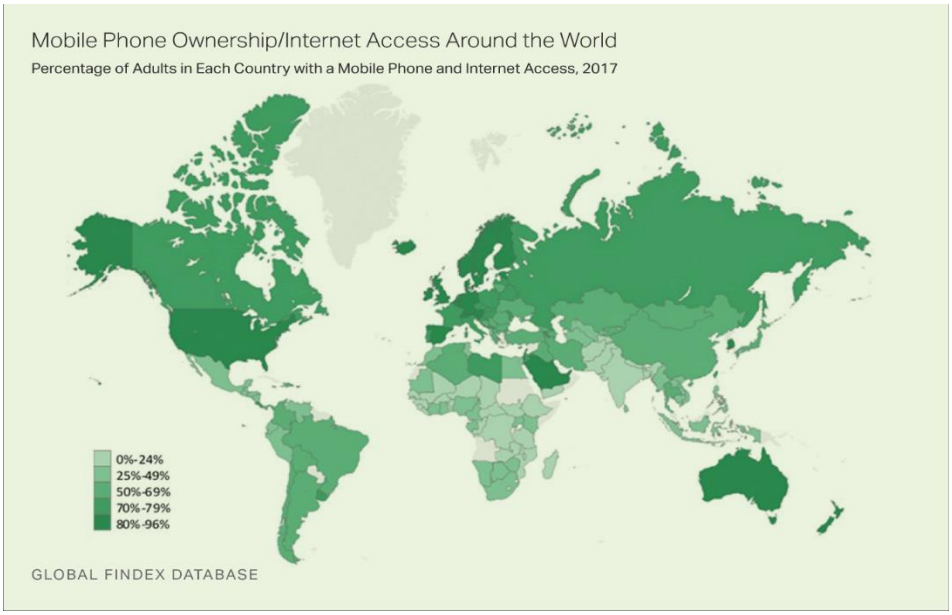
When combined with blockchain technology, P2P transactions are arguably more secure and more transparent than activities undertaken in cash, as the convenience of cash and the efficiencies that come with electronic payments are combined with the risk controls associated with pseudonymous transactions that are not otherwise dependent on a specific financial intermediary[14]. Unlike cash, crypto assets are not legal tender, and therefore not (yet) universally accepted for all goods and services, and as such, while adoption by both individuals and merchants continues to grow, conversion between virtual assets and fiat for real-world/real economy transactions is required in most parts of the world. In fact, we continue to see the growth in use, liquidity and volume of certain virtual assets being driven by the ease of convertibility especially in the case of certain more securely fiat-backed stablecoins.

[12] FATF (2016). Correspondent Banking Services. Paris: Financial Action Task Force. Available online at: http://www.fatfgafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf (accessed July 11, 2019).
[13] Self-Hosted Wallets and the Future of Free Societies; A Guide for Policymakers, November 2020; https://theblockchainassociation.org/wpcontent/uploads/2020/11/Self-Hosted-Wallets-and-the-Future-of-Free-Societies.pdf
[14] 26 https://www.coincenter.org/are-regulators-poised-to-demand-cryptocurrency-address-whitelisting-probably-not/

As P2P applications continue to evolve and propagate in the market, the ease with which transactions can be enabled between counterparties will surely evolve and directly connect individuals and entities otherwise forced to leverage third party intermediaries (who will continue to necessarily determine whether to engage them based on their risk-based approach). The growth of these systems and the connection between traditional banks and P2P networks and marketplaces will help inclusion goals while also assisting law enforcement and regulators to reinforce the societal benefits of consumer protection and personal/financial privacy while preventing illicit activity.

The Blockchain Association wrote in its November 2020 report on self-hosted wallets that "additional restrictions on self-hosted wallets would represent a disproportionate and ineffective response to the risks posed by the illicit use of digital assets and undermine law enforcement's ability to establish attribution in cases involving digital assets."[15] VASPs are enabled to conduct essential due diligence necessary to know your customer, and the auditability attributes of blockchain-enabled transactions (including those involving self-hosted/un-hosted wallets) provides additional protections both for consumers and against illicit finance risks–unlike fiat-cash transactions (e.g. USD cash transactions), which remain a higher risk for money laundering. Enabling transactions through self-hosted wallets would essentially facilitate more inclusion opportunities in the digital economy that comports with the growth of technology advancement, mobile and smartphone penetration rates, and the interconnectivity of electronic value transfer. It is worth noting that in the case of humanitarian and conflict-afflicted environments (e.g. Ukraine) the ability to enable individuals and households into digital wallets (hosted and unhosted) that can be funded with virtual assets—in particular stablecoins—provides basic income and store of value accounts as well as the ability to transact between individuals and merchants outside of formal banking. These activities are growing and enablement of KYC/KYB tools into these applications serves to ensure essential AML and monitoring controls are in place. (See Figure 2 below on mobile and internet access around the world)

Figure 2. Mobile Phone and Internet Access Around the World, 2017[16]



[15] Blockchain Association. (2020, November). *Self-Hosted Wallets and the Future of Free Societies: A Guide for Policymakers.* https://theblockchainassociation.org/wp-content/uploads/2020/12/Self-Hosted-Wallets-and-the-Future-of-Free-Societies-01.pdf

[16] https://news.gallup.com/opinion/gallup/235151/mobile-tech-spurs-financial-inclusion-developing-nations.aspx

Conclusion

Organizations operating in virtual assets, including fintech companies, VASPs, and other similar entities have traditionally fallen under the broader definition of nonbank financial institutions or MSBs/MTOs that already face enormous scrutiny by mainstream financial institutions when evaluating their respective risks related to onboarding into new accounts. These organizations have also faced regulatory uncertainty in regards to applicable licensing and consumer regulations built for businesses with a different model and that do not employ the web3 technologies that these organizations are using to democratize financial services via tokenized platforms.

Efforts to serve both regulatory/law enforcement equities and financial inclusion do not present a binary choice. Indeed, strengthening financial inclusion, including by encouraging innovation in the financial services arena with technology applications that extend beyond existing banking and payments systems can actually provide enhanced security, risk, and compliance controls, while bringing greater opportunities to marginalized and otherwise financially underserved or excluded communities and enhancing overall consumer protections. Taken as a whole, these efforts pay important dividends to stimulating proactive industry moves to create new and innovative service channels for financial services, strengthen overall AML/FCC effectiveness, reinforce the core value of a risk-based approach, and most importantly, provide opportunities for legitimate individuals and organizations that require access to the financial system to secure their economic futures.

We appreciate the opportunity to provide an industry perspective to the State of California and the DFPI in their public consultations regarding rulemaking and regulatory priorities for the web3 business environment. We remain at your disposal for any further consultation or input.

Very truly yours,

Amit Sharma
CEO, FinClusive