U.S. House Committee On Financial Services

When Banks Leave: The Impacts of De-Risking on the Caribbean and Strategies for Ensuring Financial Access
Wednesday, September 14, 2022, 10:00 a.m.
2128 Rayburn House Office Building & WebEx

Amit Sharma
CEO & Founder, FinClusive

Introduction

Chairwoman Waters, Ranking Member McHenry, and distinguished members of the House Financial Services Committee, I am honored by your invitation to testify before you today.

I am particularly grateful for the opportunity to offer counsel on issues related to de-risking in the Caribbean and to discuss its widespread impact to national and economic security in the region and beyond given the deleterious impacts of financial exclusion, and attendant consequences related to financial system integrity.

Further, I look forward to sharing my views with the Committee on the value of new technology capabilities and innovation taking place both inside and outside the traditionally regulated financial services industry, and in particular in the leveraging of blockchain technology applications and virtual assets that can play an important role in addressing de-risking and drive equitable and safe financial services access—especially to particularly vulnerable groups and in need of secure financial tools and services.

Overview

Several important trends are important to recognize as we look at the evolution of financial services and the manner and methodology employed by many individuals and entities to financially and commercially transact between each other.

The first is the recognition that there has been, and continues to be, an exponential increase in financial intermediation taking place outside traditionally covered or regulated channels. These include, but are not limited to, peer to peer (p2p) transactions, the extension of credit and provision of lending by institutions (or individuals) to other institutions and individuals directly and without regulated intermediaries, the growth in mobile and web-based banking and financial services, the increasing 'digitization' and 'tokenization' of financial instruments and assets (e.g. cash, stored value, marketable securities, etc.) and the growing 'virtual asset services' sector. Under any rubric, we are seeing financial innovation blossom. Some of these efforts hold tremendous promise, while others may present addressable risks, and still others, unfortunately, look to deliberately circumvent or avoid the basic fundamentals of prudent financial intermediation.

Secondly, the growth of financial activities *outside* of traditionally regulated channels particularly noteworthy and provides tremendous opportunity to increase access for the globally underserved, unbanked, underbanked and those otherwise financially excluded, including those we would consider simply 'poorly' banked. Such efforts have understandably given financial regulatory agencies pause as nonbank financial services providers and other non-traditional finance companies have emerged into the formal financial services sector. Technology and social media companies, online/e-commerce retailers, marketplaces and crowdfunding platforms, corporate entities with large recurrent user/consumer populations, and others with large and growing affinity groups are increasingly realizing the commercial potential of providing financial products and services through their infrastructure and existing networks. While these efforts provide great promise in reaching traditionally underserved/excluded populations, doing so without essential safeguards to safety, soundness, consumer protection and financial system integrity could indeed lead to broader and systemic risks or the facilitation of illicit activities to which the BSA and other US regulations governing AML/CFT are intended to address.

Finally, since the tragic events of September 11, 2001, and exacerbated by the credit and financial crisis of 2008, a growing body of regulations and financial oversight rules have understandably caused consternation among financial market participants – traditional and non-traditional alike – working to adhere to these guidelines. With an average governance/risk/compliance (GRC) spending of greater than 25% of their operating budgets on regulatory costs, global banks have faced the 'economic' reality of servicing otherwise labelled "high perceived compliance risk" individuals and entities or suffering the consequences of regulatory fines and punitive measures for lack of demonstrably strong AML/CFT controls. Further, new entrants to the financial sector face consequential costs in their efforts to ensure their risk and compliance controls, policies and procedures, personnel, and relevant regulators and supervisors—in some cases numbering greater than 50 in the nonbank money services business sector—are appropriately engaged and in place to undertake activities that would serve broader financial inclusion initiatives, but nonetheless face both a diverse and less-than-clear regulatory landscape, as well as a lengthy and costly approval process to undertake their activities.

By no means do I sympathize with those institutions that have willfully chosen to turn a blind eye to money laundering, sanctions evasion, terrorist financing and other illicit activity, or underinvested on foundational AML/CFT controls. However, we are indeed seeing the consequence of growing regulation and the associated economic consequences stemming from "de-risking" or the jettisoning of business otherwise considered "high perceived compliance risk." Such efforts have unfortunately fallen disproportionately on those constituents– individuals and entities—whose financial engagement and access is essential to building economic resilience, and sustainable financially responsible behaviors—the US and global poor, international remittances, humanitarian assistance and charitable works, and international correspondent banking, among others—all examples of de-risking and a lack of inclusive financial opportunities in the Caribbean and indeed in many other parts of the world.

Indeed, even in the face of specific national security threats and challenges the US Government and its allies across the world face, the use and propagation of alternative financial service applications including virtual assets, blockchain enabled value transfer systems, decentralized financial services protocols are showing to be a rapidly growing and useful set of solutions. Where many traditionally financially marginalized populations are unable to engage with formally regulated banks, web-based applications that enable individuals, households, small businesses and even whole governments (e.g. Ukraine), are able to raise money and transact digitally -- providing a viable and scalable alternative when formal channels for financial access are no longer available. The good news is that the technological and operational infrastructure enabling such access carry with them the very attributes that enable consumer protection, traceability of transactions, verification of identity, and ultimately to build and extend economic resilience.

The manner in which financial exclusion has grown in the Caribbean and the attendant risks of 'de-risking' due to ongoing AML/CFT uncertainty amidst a growing trend of nontraditional and technology-led initiatives to provide financial services, behooves us to look at this obstacle in a fundamentally new light and to find ways in which new technology can in fact drive financial inclusion and provide secure and equitable gateways to essential financial services, while they strengthen financial sector integrity in tandem.

The Importance of Financial Inclusion

It is important to reinforce the critical issue of financial inclusion, as access to financial services is vital to building economic resilience and strengthening overall financial health. The financially excluded or underserved stretches beyond the world's unbanked or underbanked individuals. Millions of small businesses, entrepreneurs, and organizations considered or labeled 'high compliance risk' by governments and global AML/CFT standards can also cause financial institutions to 'de-risk,' or deny or cease servicing such customers. Unfortunately, de-risking has also disproportionately impacted certain segments of the global economy where secure access to services is the lifeblood for many. De-risking is particularly problematic for:

- Certain types of customers: LMI (low to moderate income) and those without verifiable identification, the global poor, or those without a discernable or recorded financial or credit history;
- Certain types of businesses considered 'high perceived compliance risk,' which include: money services businesses (MSBs), money transfer operators (MTOs) and other remittance providers; nonprofit institutions and NGOs/IGOs, especially those working to deliver aid and assistance to areas of distress or conflict; international correspondent banks (especially those in emerging markets);
    - Importantly, the growth of fintech and virtual asset services providers, or VASPs, are now in the crosshairs of financial regulators, as these emerging and rapidly growing financial market participants and technologies engaged in alternative financial services are increasingly engaged in activities historically driven by mainstream bank financial institutions; they also provide valuable avenues for financial inclusion, and are powered by technology stacks that

actually serve to mitigate certain risks and present more efficient and transparent operations that can serve to strengthen intended AML/FCC controls; and
- Certain types of jurisdictions: emerging or frontier markets and/or those considered to have weaker AML/CFT regimes, financial system regulatory oversight controls, or otherwise challenged with systemic corruption.

These institutions, individuals and jurisdictions struggle to access formal banking relationships to simply hold and transfer value—the basic fundamentals of banking. These fundamentals enable individuals (and organizations) to improve their financial lives as they are related to the ability to spend, save, borrow, transact in society, and financially plan one's life. Financial inclusion activities enable as many people and organizations to engage in the formal economy, and must be facilitated with a confidence that their financial assets will be safe from theft, accessible to them when, where and in a manner they need, and transferable to those with whom they must personally and commercially interact.

Financial inclusion also pays dividends to the excluded and underserved as well as society as a whole. Simply including the unbanked in the formal financial sector can significantly help the global economy by reducing transactions in the black or unregulated markets and expose exploitative behavior and labor practices. With a growing reliance on remittances from more developed economies such as the U.S and Western Europe, many frontier markets receive upwards of 1/3 of their GDP from such flows. In fact, remittances make up more than three times the size of international development assistance (IDA).[1] Some estimates show that banking the unbanked would lead to a $600 billion rise in the worldwide economy per year, generate $4.2 trillion in new deposits, create 95 million new jobs and drive an estimated $3.7 trillion in global GDP growth.[2]

Financial inclusion is also a critical first step to building financial health. This is a common goal for populations in developed and developing economies alike. Too often, financial exclusion is (mis)understood to only impact the global poor in developing and frontier economies, but the challenges of financial exclusion impact even those in the U.S., one of the wealthiest nations on the planet. Statistics in the U.S. itself serve to illustrate this point:
- Approximately 25% of the U.S. are un- or under-banked—lacking secure and sustainable access to mainstream financial services;
    - Similar to global statistics, these numbers reflect individual financial exclusion and do not include the thousands of businesses (especially small and medium enterprises (SMEs) that represent 99% of all U.S. businesses) and entrepreneurs that lack access to credit and lending products to establish and grow their operations;
- Almost 2/3 of U.S. persons cannot handle an unintended expense of $400 or more;

[1] Migration and Remittances (worldbank.org); https://www.worldbank.org/en/topic/labormarkets/brief/migration-and-remittances

[2] https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Employment%20and%20Growth/How%20digital%20finance%20could%20boost%20growth%20in%20emerging%20economies/MGI-Digital-Finance-For-All-Executive-summary-September-2016.pdf

    - These include resulting out-of-pocket expenses such as an unexpected health event, a breakdown of a vehicle needed to commute to work or a house maintenance expense, which dries up minimal savings;
- Greater than 50% of the U.S. struggle with daily and weekly expense management;
    - The single most important driver of financial health is the ability to responsibly financially plan for one's future.

Beyond individual statistics, the impacts of financial exclusion in the small business community, including organizations considered to be small and medium enterprise (SMEs) is larger than many think. Formal SMEs represent approximately 90% of global businesses (note that 99% of all US companies are small businesses[3]), and more than 50% of official employment. The reality of financial exclusion grows when one includes informal or micro-businesses as well; according to the International Finance Corporation (IFC), 65 million organizations (40% of such organizations) in developing countries fall $5.2 trillion short of their financing needs every year. In the emerging markets, SMEs are also responsible for 70% of new jobs, but these companies are less likely to be able to obtain formal bank lending or access basic credit facilities.[4] When the majority of entrepreneurial ventures are essentially one- or two-person/family-based endeavors, financial access is more practically determined by individual characteristics and background vs. the organization itself. Ensuring that individual financial access issues are enabled directly can contribute to one's ability to start and grow their own businesses, employ others and grow their individual, household and community wealth.

De-risking presents an unfriendly obstacle to individuals, organizations, and jurisdictions in need of institutional support as some of the most financially vulnerable but economically essential members of the global market. The financial exclusion afforded by the de-risking approach cripples commerce through the systemic denial of access to financial solutions that are indispensable to growth. The good news is that with the growing reach of mobile and web-based technology applications working to connect individuals, households and businesses in the global economy, the advancements in commerce and digital access continue to enable more connectivity—even in some of the world's frontier and remote marketplaces. Smartphone penetration and adoption rates continue to increase, which enables connectivity for financial services that are much more capable today than five or ten years ago.[5] While access challenges continue to be addressed as more connectivity is enabled, ensuring safe and equitable access to financial services—those that can be assured with data privacy and economic security controls remain an ever-growing need.

The institutional response should not be wholesale deregulation, but innovation in pursuit of the most efficient and developmentally stimulating allocation of resources that serve to broaden financial access while maintaining financial system integrity and consumer protections through a rapidly evolving financial technology and, in some cases, exclusively web-based environment.

[3] https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf
[4] https://www.worldbank.org/en/topic/smefinance
[5] https://www.statista.com/statistics/203734/global-smartphone-penetration-per-capita-since-2005/

Modern Institutional Challenges Aggravated by De-risking

In the current environment resulting from the COVID-19 pandemic, issues of financial exclusion and challenges related to a lack of access to financial services and the ability for organizations and individuals otherwise excluded by formal financial services have come in stark relief. As discussed previously, de-risking has disproportionately impacted certain segments of the economy with profound consequences to their ability to ensure their own financial stability and economic security. Tools enabled by blockchain technology in both regulatory compliance and cross-border payments play an essential role in addressing these challenges, which have manifested in many areas, specifically including:

- Ability for small businesses to engage financial services and support through the Paycheck Protection Program (PPP)–Banks need a streamlined and efficient process to take in, process and conduct due diligence on these organizations as well as ensure on an ongoing basis that such attributes that have supported their application remain in the months ahead when such programs are executed and funds are provided and accounted for by participating financial institutions.
- Financially excluded or underserved individuals and organizations like those noted above are often considered to be of 'higher perceived risk' by traditional financial institutions. Tracking their payments and ensuring auditability of client and transaction data becomes especially important; blockchain tools can play an important part as they can support digital identity applications to strengthen KYC/KYB requirements and transactions-based analytics.
- Ability for individuals to receive ongoing stimulus or economic support checks as part of federal and state-based programs, where they may not be in formal banking relationships, but do engage in alternative financial products including digital/virtual-asset related services.
- Ability for individuals and companies to facilitate cross-border remittances, which have been impacted by the pandemic. Analysis shows migrant workers were impacted as many were sending less money home (e.g. South Asia, Africa, Latin America) and are beginning to see more monies needed back in the US. This reversal of overall flows flexibly (through multiple channels, including digital/crypto) and securely will be a lifeline to families, households and businesses.
- Nonprofit and charitable organizations – including those engaged in COVID-19 response and relief efforts struggle to maintain financial services to include accounts (store of funds), operations (financial operations and treasury management), and payments (sending needed funds to beneficiaries in need in a timely and secure manner). Blockchain-enabled value transfer systems serve to connect counterparts globally and securely with near-real time payments capabilities and transparency/auditability of transactions to ensure funds are both sourced from legitimate parties and sent to/received by intended beneficiaries in need.

De-risking limits opportunities for financial inclusion in these areas, further disparaging underserved populations. For example, humanitarian organizations reported that they have lost access to financial services as a result of de-risking. This restricts humanitarian assistance to refugees from political conflicts or natural disasters that could prevent life-saving aid from reaching those experiencing starvation, exposure, and/or disease.

According to the FATF – "De-risking affects services and products, financial institutions and other agencies. The most severe effect of de-risking in the Caribbean has been the termination of correspondent banking relationships which includes check clearing and settlement, cash management services, international wire transfers, trade finance and conducting foreign currency denominated capital or current account transactions."[6] According to the Center for Statistics & International Studies, "a survey in 2017 by the Caribbean Association of Banks found that 21 of the 23 banks in 12 Caribbean countries had lost at least one correspondent banking relationship. The impact was particularly hard on countries in the Eastern Caribbean (in particular Antigua and Barbuda and St. Kitts-Nevis), Suriname, and Belize."[7]

De-risking increases costs, financial exclusion, and mistrust for the end user and drives financial transactions underground to unregulated channels. These channels do not necessarily follow best practices or abide by regulatory obligations introducing more anonymous banking and unmonitored or reported money laundering or terror financing activities. Ironically, achieving the polar opposite of de-risking aims. This pushes financial services from the regulated entities directly to the higher risk unregulated entities that can afford to provide unregulated financial services or hawalas.

The Council of Europe finds de-risking unacceptable within the framework of FATF standards in its termination of entire classes of customer relationships without thorough risk analysis. Such compartmentalization manifests itself in the unwarranted financial exclusion of individuals and organizations, notably NGOs.

The Value of Blockchain Technology in Financial Inclusion

There are several areas in the regulatory compliance and payment space that can be enhanced by the use of blockchain technology. The foundational attributes of this technology helps build and reinforce trust and provides transparency and security in ways that traditional bank and nonbank financial institutions can leverage to enhance both value transfer as well as financial crimes compliance (FCC) controls and activities.

Briefly, those attributes include:

- *Immutability* – participants in a network are unable to change or tamper with transaction or client data after it has been recorded to the shared ledger. This attribute has application in enhancing know your customer/know your business (KYC/KYB) verifications to manage ongoing customer information and attributes as well as transaction-level data

[6] De-Risking (cfatf-gafic.org)
[7] https://www.csis.org/analysis/there-new-normal-de-risking-caribbean

(payments and transfers of value) for appropriate transaction monitoring and associated risk scoring and analytics.

- *Distributed/Decentralized* – Governance is spread across participants in a particular network such that information/data (transactions, contracts, value, client information) can be accessed by participants in a network no matter where located, lessening concentration risks of control of important data, and providing transparency related to such data without having to uncover the particulars of the data (sensitive personal identifying information). This incentivized self-governance can be provided both through public blockchains as well as private or federated blockchains.
- *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.
- *Security* – the encrypted and distributed nature of blockchains alongside the immutability of the ledger, allows for the preservation of underlying data or assets being transacted to maintain security controls and needed protections. As information is hashed cryptographically on the blockchain, the true nature of the data (sensitive PII or transaction data) can be protected, but results, outcomes or other verifications of such data can still be provided—to regulators, counterparties, law enforcement or others.

One of the most visible and growth-oriented areas in the application of blockchain technology is in the increasing issuance and use of virtual assets, generating new ways of creating, storing, and transferring value over the internet. Virtual assets have the potential to enable the creation and movement of value between counterparties directly, and over an internet infrastructure that does not necessarily require intermediaries to do so. Stablecoins, including and in particular those collateralized, backed, pegged or represented by fiat currencies or other 'stable' assets represent an additional value of extending the reach of economic value to counterparties in need. These innovations serve to reinforce the additive nature of virtual assets to the formal financial services economy while reinforcing the power of capital and financial markets—such as the US in the case of US-dollar backed stablecoins—which form an additional extension of positive influence of the US to its global neighbors.

What has been the purview of a few large technology companies enabling access to such tools and services, can now increasingly be accessed, created, and maintained with open-source code and technology applications that reward these infrastructure providers, that tokenize value that is increasingly fungible and enabling of everyday commerce. These innovations represent the next frontier of web-based applications that can be truly peer-to-peer, and enable commerce across jurisdictions directly between counterparties and built on the attributes described above that serve to enhance system transparency and integrity, while enabling global access.

The aforementioned attributes, when applied in the case of underlying financial inclusion initiatives, can help make the world a more transparent, efficient, and frictionless place.

Importantly, blockchain enabled networks and digital assets have the ability to reduce some of the obstacles to providing efficient and affordable access to financial services to the millions of people in the United States and billions around the world that are underserved or excluded from the formal financial system. This is especially true given the growth in financial activities being undertaken by nonbank financial institutions. In, fact these non-bank nonfinancial institutions (e.g. charities and crowdfunding platforms, e-commerce companies, social media and technology companies) realize that their networks provide an easy-to-engage set of constituents to whom they can offer select financial services (storing and protection of funds, transfer of funds, access to funds, etc.) as long as those activities also ensure coverage of their FCC obligations to which 'covered' financial institutions are already subject.

Despite this potential, the widespread adoption of this technology by financial institutions, particularly to address the challenges of financial inclusion, remains slow due to the perceived associated risks and lack of clear and consistent regulatory guidance—reflecting both jurisdictional differences in approach and pace of adoption, and, as is the case in the United States regulatory environment, differences in approach by and between different functional regulators related to the institutions and activities they explicitly oversee. As a result, non-traditional entities and organizations less constrained by outdated regulations and technology have stepped into to make it easier, faster, and cheaper for people to fulfil their fundamental financial needs of creating, storing, and transferring value.

The decentralized and frictionless nature of virtual assets provides both an opportunity and a challenge to regulators and financial services providers alike. Financial regulators should embrace the myriad of opportunities this new technology is generating and tackling head-on the financial crimes risk associated with applications that leverage this technology through modernized FCC governance addressing one's *activities and practices* regardless of the type of entity or jurisdiction of domicile. Part of that effort should include a recognition of the attributes of blockchain technology that in fact make it easier in many ways to identify, track, and disrupt the illicit use of funds, while they also provide new mechanisms to provide banking and payments products in a new way—especially to financially underserved, excluded or marginalized populations and in furtherance of US national and international security and economic interests. Some notable examples of the use of virtual assets and capabilities afforded by blockchain technology include:

- Enabling marginalized communities (including those in areas of conflict or humanitarian strife) to be furnished digital wallets into which virtual assets—including USD-backed stablecoin—can be funded that enable access to vital economic resources and the ability to engage in peer-to-peer transactions between individuals and merchants providing essential services,
- Providing donors globally to provide needed funds quickly and directly to recipient organizations and individuals directly and without the complications associated with accessing cash or other fiat instruments,
- Ensuring know-your-customer (KYC) controls on digital wallets to remotely verify and validate individuals and businesses securely,

- Incorporating essential transaction monitoring and analytics on transfers of digital assets between counterparties seamlessly and without compromise to personal data,
- Issuing digital identity credentials to users of wallets and virtual assets that can serve to verify those users, perform essential screens (e.g. sanctions checks), and trace transactions to ensure their legitimacy and security against exploitation by illicit actors.

There are several important innovations that serve to enable financial inclusive opportunities that also related to the requisite financial crimes compliance objectives the sector and regulators and policy makers would like to see to help protect consumer safety and privacy and overall financial system integrity.

Bringing Technology To Bear–Addressing Identity Challenges Amidst Increasing Globalization and Digitization of Financial Services

Identity has long played a central role in the financial services industry as access and financial system protections revolve around the central question of know-your-customer (KYC). KYC controls are based on the appropriate identity management and verification systems necessary for a financial institution's effective customer due diligence (CDD) and customer information program (CIP). Specifically, the focus of identification (establishment, authentication, and authorization) enables financial intermediaries (e.g. financial institutions, custodians or value transfer operators) to tie the property/assets (store of value) to be facilitated for a person associated with an established identity.

Identification is based on resolution of an identity, which assures the bona fides of a person using trusted, reliable sources of information to achieve confidence that not only the person exists, but that institutions are in fact also engaging (providing services to or interacting) with that specific person. The strength of the identification process directly contributes to the integrity of information which is relied upon to discern whether that specified person is connected to potential proceeds of crime and/or to untangle potential proceeds of crime from legitimate property.

As such, global guidance for KYC includes applications of both traditional identity management and verification activities and are increasingly incorporating more recent applications of digital identity systems, because the importance of identity management and verification is central to financial institutions' assurance that they are doing their part in keeping their institution—and the financial system more broadly—closed off from illicit actors. It is in this vein that global standard setters, such as the Financial Action Task Force (FATF), apply extensive guidance related to KYC to address anti-money laundering/counter-financing of terrorism (AML/CFT) and financial crimes compliance (FCC).

FATF has offered this specific guidance on digital identity: "using reliable, independent source documents, data or information…that provide an appropriate level of trustworthiness."[8] Through

[8] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf

the review of how to assess the strength of identification, a risk-based approach can be used within digital identity tools to apply the right level of risk mitigation. This can be done by reaching out to newly available, trusted sources of identification (e.g., utilities, financial institutions, etc.) to meet the needs of the relationships that financial intermediaries have with clients and counterpart financial institutions. In fact, in light of the global COVID-19 pandemic over the last two years, FATF has further and explicitly noted that digital identity solutions and related technologies should be explored to aid and modernize financial services while managing illicit finance and security risks.[9] Dynamic expansion of the approach to such modernization is needed to address growing financial access concerns.

Globally, between 2.5 and 3.5 billion people are considered unbanked or underbanked. According to the World Bank, 1.7 billion adults (over 30% of the global population), are fully unbanked, which means that they do not have an account at a regulated financial institution or have funds/stores of value in an equivalent mobile money account.[10] This has a significant impact on their ability to maintain, let alone strengthen, their economic resilience.[11]

Unfortunately, the majority are disproportionately low or moderate income (LMI) or considered poor, exacerbating their inability to build financial wealth and improve their financial condition. Often it is the lack of a verifiable identity—understood most often as the proof of a government or federally issued identity—that prevents these individuals from being able to establish a bank account. The KYC and AML/CTF checks that banks are required to conduct before onboarding new customers pose a key hurdle to this verification.

As a result, for the more than 1 billion people that do not have a specific form of legal identification, financial access remains nearly impossible. Further, institutions are obligated to monitor their customers to ensure that their identity information (e.g. identification numbers, physical address, phone number, etc.) remains current. Failure to do so allows hackers, cyber criminals and other illicit actors to break into accounts and take over financial assets. This is particularly an issue in the United States (and many western countries) where overreliance on static personal identifying information (PII) exacerbates the identity management process in many financial institutions, resulting in the following problems:

- New account opening is difficult for many institutions, and losses from new account fraud have continued to remain high.[12]
- The U.S. Federal Reserve reports that synthetic identity fraud (fake names associated with real individual identity numbers such as personal passport, driver's license, or social security numbers) is costing U.S. lenders $6 billion annually and is the fastest growing type of financial crime in the U.S.[13]

[9] http://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html
[10] https://globalfindex.worldbank.org/
[11] Ibid
[12] https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-study-fraudsters-seek-new-targets-and-victims-bear-brunt
[13] https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf

- Between 2017 and 2018, the volume of PII data exposed in data breaches increased by 126%, with more than 446 million records exposed.[14]

Also unfortunate is the global economic tendency to rely on paper-based identity proofs such as government-issued forms of identity. As financial services become increasingly digital, this "identity gap" between digital and physical identity documents continues to hamper access to digital payments and online financial services.[15] This is true for both developed and less developed economies. Digital identity solutions such as verifiable credentials technology can offer strong avenues of development to build more accessible and secure identification in order to bridge the gap.

Digitally Verifiable Credentials

Verifiable Credentials form the foundation for verifiable data in the web of trust. They can contain many different types of information as well as different types of credentials. Many software providers, private & public institutions, and a wide range of businesses are implementing this technology in their offerings.

Traditionally, regulated bank and nonbank Financial Institutions (FIs) run their own KYC, KYB and various levels of CDD and EDD for the subjects that would like to use their service offerings according to the risk profile of each subject. There is often hesitancy towards such reliance on 'third-party' KYC/KYB verifications, and thus there is no sharing or re-use of the corresponding results of the KYC/KYB and other screens associated with these clients between FIs. This ultimately serves to increase the cost and time to onboard a subject to the FI or revalidate subjects that may have already been screened and/or verified by previous KYC/KYB efforts and/or as part of the subjects' FI's customer information program (CIP).

To solve the sharing and reuse of compliance information without divulging the PII/EII, multiple efforts are underway in the marketplace to design digital identity issuance and validation protocols that 1) provide a verifiable proof of one's identity, and 2) enable control of underlying PII information by the user. Taken together, such verifiable credentials can be used to validate the authenticity of an individual (or a business), its level of risk as is necessary to be defined by regulated financial services companies on their customers and counterparties, and the explicit due diligence elements verified to comport to the level of that clients' risk.

FinClusive has developed and implemented a service called 'CDD Check Connect'. CDD Check Connect facilitates via a multilateral information sharing agreement between different partners and customers leveraging the FinClusive Compliance as a Service (CaaS) platform; thus enabling the FIs, whether or not they are customers of FinClusive, to share the compliance data securely and verify the credentials associated with subjects run through KYC/KYB.

[14] https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf
[15] https://morningconsult.com/opinions/the-future-of-identity-in-financial-services-threats-challenges-and-opportunities/

Further, the level of due diligence as determined through the subjects' risk profile further delineates the risk associated with a client and can include levels and types of due diligence ranging from 'basic' (e.g. name match and sanctions screen) to 'enhanced' (e.g. social and adverse media, source of wealth, etc.). This multilateral agreement structure has been updated and refined to include standardized language of an AML compliance 'reliance agreement' which is constructed to enable the following:

- a third-party FI can 'rely' on the KYC/KYB/compliance processes of another FI (which would be FinClusive itself or another customer of FinClusive leveraging FinClusive's compliance applications and global KYC/KYB and CDD/EDD toolkit; and
- the ability to reinforce use and value of a common framework for FCC compliance and KYC/KYB processes both through its technology application as well as its governance and global AML/FCC policy formulation which comports to international standards.

The FinClusive CaaS platform embeds the decentralized identity/verifiable credential through the KYC/KYB processes, creating a unique identifier termed 'FinCID', which is connected to all of the subject's data stored in the platform. The subject's data includes both the attributes run through due diligence and background screening as well as evaluation based on their level of risk, as well as all of the transaction data generated by various platform services during the lifecycle of engagement with the subject. This includes transactional data associated with digital wallets belonging to or under the control of the subject. The FinCID is constructed such as to be able to be 'attached' to any 'client related attribute' from:

- the client's underlying personal identifying information/entity identifying information (PII/EII),
- the client's account details, digital wallet details, or other relevant account/transaction facilitation information,
- transaction data and flows, and
- affiliate data (counterparties with whom they transact, etc.)

Traditionally, regulated bank and nonbank Financial Institutions (FIs) run their own KYC and KYB and have various levels of customer due diligence (CDD) and enhanced due diligence (EDD) for the subjects that would like to use their service offerings based on their risk profiles. There is often hesitancy towards such reliance on 'third-party' KYC/KYB verifications, and thus no sharing or re-use of the corresponding results of the KYC/KYB and other screens associated with these clients between FIs, which serves to increase the cost and time to onboard a subject to the FI or revalidate subjects that may have already been screened and/or verified by previous KYC/KYB efforts and/or as part of the subjects' FI's customer information program (CIP). This is where the CDD Check Connect solution creates value; enabling the sharing and reuse of compliance information without divulging PII/EII.

Conclusion: Financial Inclusion as a Matter of National Security

I am hopeful these examples show how technological advancements in web-based infrastructure, tokenization of value, and digital identity—leveraging blockchain and distributed ledger technologies in particular—can serve to address ongoing de-risking challenges and strengthen and modernize AML/CFT efforts to drive financial inclusion.

In sum, we must look at the tools we have created to drive financial inclusion, community-based financial engagement, and risk-based approaches to financial facilitation that ultimately bring more activity to regulated financial channels. New technologies, including in advanced analytics, mobile and digital banking and distributed ledgers, can serve to provide additional financial engagement highways that are more easily accessible and afford the essential protections (in both privacy and personal data as well as personal financial assets) that remain inherent challenges to many financially underserved and excluded parties from securely engaging the financial system. These same technologies can serve to dramatically decrease the friction, redundancies and inefficiencies of the AML/CFT activity set while preserving the essential controls inherent in facilitating safe and secure financial intermediation.

The United States has one of the most effective AML/CFT regimes in the world. As we have relied more on this regime to address various threats to our national and collective security, our efforts are increasingly undercut by the misinformed and false binary choice between driving financial inclusion and protecting our financial system from abuse by illicit actors. New technologies at work today have the power and capability of addressing "actual" vs. "perceived" risk, strengthening coordination among and between financial market participants and intermediaries (both traditional and non-traditional) as well as financial regulators and law enforcement, and provide gateways for access in ways that can strengthen financial system controls for the many licit and otherwise legitimate activities and participants we need the system to serve, while strengthening the ability to identify and root out illicit activities.

These realities in financial and technological infrastructure force us to rethink and innovate financial inclusion opportunities and the attendant AML/FCC considerations in a new light. The increased globalization of finance, whereby counterparties can interact on an open-web-based platform in a peer-to-peer context without a specific regulated financial services intermediary with explicit regulatory and supervisory obligations, requires this new thinking as they provide gateways for financial inclusion and potential solutions to pressing development and national security goals in tandem.

These gateways and technologies can bring down barriers to access while preserving essential safeguards for traditional and non-traditional financial market participants. The strength of United States globally is founded on, among other things, a strong and unparalleled financial and economically resilient infrastructure. Extending this to the more than 25% of the country's financially underserved and excluded—and ultimately to the 2.5-3 billion people globally underserved or excluded—including and especially our global neighbors—ultimately serves to drive overall financial system integrity and security moving forward, but also underpins our collective national security both at home and abroad.