Promoting Corporate Transparency: Examining Legislative Proposals to Detect and Deter Financial Crime

Subcommittee on National Security, International Development, and Monetary Policy
(Committee on Financial Services)

Amit Sharma
Founder and CEO, FinClusive
March 13, 2019

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.

In particular, I am grateful for the opportunity to testify in support of several initiatives this committee and Congress are pursuing to modernize the anti-money laundering / counter-terrorist financing (AML/CFT) regime of the United States, and the attendant issues emanating from the U.S. Bank Secrecy Act (BSA) to strengthen the integrity of our financial system, and importantly recognizing the value in new technology capabilities and the innovation taking place within and outside the traditionally regulated financial services industry that can also drive financial inclusion.

Congressional efforts to strengthen and codify engagement between the regulatory community and the financial services industry – taking into consideration the growth in particular in the non-bank financial institutions sector and exploding financial technology (fintech) and regulatory technology (regtech)—is of paramount importance given the ever changing nature of technology and the applicability of some of these important advancements to not only aid in strengthening regulatory compliance associated with the BSA and broader AML/CFT, but also importantly and significantly, such efforts can and would support financial inclusion as doing so has a direct benefit to our collective national security.

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 (phone and web-based) banking, the increasing 'digitization' and 'tokenization' of financial instruments and assets (e.g. cash, stored value, marketable securities, etc.) and the emerging and growing 'crypto-currency' sector. Under any rubric, we are seeing financial innovation blossom, where traditional financial market participants—and increasingly non-traditional entrants, are innovating in both the form of, and manner in which, counterparties are engaging in modern financial engagement, asset building and wealth creation. 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 prudential financial intermediation.

Secondly, the growth of financial activities *outside* of traditionally regulated channels is also noteworthy and provides tremendous opportunity to increase access for the globally underserved, unbanked, underbanked and those otherwise financially excluded. Such efforts have understandably given financial regulatory agencies pause as nonbank entities and other non-traditional finance companies have emerged into the financial services sector. Technology, social media, online/e-commerce retailers, 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, 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 a growing body of regulatory and compliance requirements. With an average governance/risk/compliance (GRC) spend of 25% of their operating budgets, global banks have faced the 'economic' reality of servicing otherwise labelled "high perceived compliance risk" individuals and entities or suffer the consequences of regulatory fines and punitive measures for lack of demonstrably strong AML/CFT controls. 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 in 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 serve as 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.

The manner in which financial exclusion has grown in the last two decades, and/or the myriad and diverse reasons that exacerbate financial exclusion, are far beyond this testimony, however, 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 these market participants in a fundamentally new light – and find ways in which new technology can in fact drive financial inclusion and strengthen financial sector integrity in tandem.

Supporting Innovation and Technology Advancement in Financial Sector Integrity and Inclusion

Financial innovation has continued to grow exponentially in the last decade. The advent of new technologies such as mobile and digital banking, alternative payments, advanced analytics (including artificial intelligence (AI) and machine learning) and distributed ledger technologies (DLT), have expanded opportunities never before afforded to financial market participants. Importantly, such technologies give us ability and insight in reducing friction and oftentimes redundant processes (especially as related to know-your-customer / customer-due-diligence (KYC/CDD) and ongoing monitoring), dramatically increasing analytics and processing speeds within a traditionally 'man-hour'-centric compliance environment (aiding investigations, law enforcement coordination and reporting), and improving information sharing by and between financial intermediaries, regulators and law enforcement while protecting essential data and personal identifying information (PII).

For example, AI and machine learning capabilities have the potential for driving enhanced and bespoke analytics related to targeted investigations or specific illicit finance typologies (e.g. human trafficking-related financial activities or sanctions evasion) in financial institutions. Many new regulatory technologies have added tremendous value to financial institutions to ensure compliance officers and teams the ability to carry out 'look backs,' suspicious transaction reviews, enhanced or targeted investigations and the like, to specific money laundering and illicit finance typologies where human-centric reviews and analysis can be both cumbersome and expensive endeavors.

More routinely, however, distributed ledger technology (DLT) has emerged as an additional potential value additive capability that has tested application to both driving secure, cost-efficient payments 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. There is no central administrator or centralized data storage. Blockchain is one form of DLT that uses independent computers (referred to as nodes) to record, share and synchronize transactions in their respective electronic ledgers (instead of keeping data centralized as in a traditional ledger). There are several characteristics of DLT – in particular, blockchain, that facilitates 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.
- Immutability: 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. The near-real-time settlement functionality can facilitate near real-time payments between counterparties vs 3-5-day settlement times via traditional channels. Transaction history and specifics cannot be altered once inputted. 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 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 assist network participants in a common financial ecosystem.

While the applications for DLT are far reaching, one can easily see where it can add value in particular to underserved/excluded markets as well as in the furtherance of AML/CFT goals. Responsible and disciplined application testing and deployment of such technology alongside regulatory oversight would indeed pay dividends to the industry, regulators and law enforcement alike.

Codifying Regulatory Commitment to Financial and Regulatory Technologies

As an initial observation, I commend the regulators and their joint statement made in December, 2018 to support innovative efforts to combat money laundering and terrorist financing. That statement, while necessarily not an endorsement of any specific kind or type of technology, reinforced to both the traditional banking community as well as the growing fintech and non-bank financial services community of the important role new technological advancements can make in streamlining AML/CFT processes, ensuring cost effective and frictionless approaches for financial services participants of all types – with and through banks and non-banks alike – and in effort to keep the financial system safe and secure from illicit activities.

While the statement was an important start, a statement alone is not sufficient in delivering practical and tested solutions to the financial services industry without proactive, ongoing, dedicated and funded support by financial regulators directly. Moving to make this innovation guidance more permanent

through concrete mechanisms by individual regulators and across them collectively, and that directly engage both financial services institutions AND technologies in their application to AML/CFT, will pay important dividends. It is worth noting that in large part, fintech companies and other non-traditional nonbank financial institutions very much want for their operations and activities to comport with essential financial system integrity safeguards, and that their efforts meet the attendant goals of driving both commercial opportunities as well as ensure risk is appropriately understood and managed within the financial sector. While there are indeed those companies, rogue individuals and efforts in non-traditional financial service channels that deliberately look to avoid regulatory scrutiny or oversight, my comments today reflect instead the broader majority of enterprises looking to provide financial intermediation, products and services in a way that enhances transparency and that are attendant to the inherent compliance risks associated with the financial sector.

Connecting Financial Inclusion to Ongoing AML/CFT Modernization and Financial Sector Resilience

As discussed above, we encourage stronger, codified and financially and legislatively supported private-public cooperation in the application of new technology to financial system integrity – in particular in the modernization of the United States AML/CFT regime. There are several ways we encourage this 'permanency' of the December statement by the regulators; below are several concrete and practical efforts that would indeed be welcome by industry participants – whose goals are indeed shared to drive a more transparent and safe financial system that is also inclusive.

- Creation of Dedicated Technology / Innovation Units and Coordination Centers:
    - We encourage Congress to mandate, authorize funding for, and support the creation of dedicated technology/innovation centers driven individually by regulators – in particular the Office of the Comptroller of the Currency (OCC), the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of Federal Reserve, and the National Credit Union Association (NCUA). Each of these regulators differ in both their mandate and jurisdiction, and as such, have a unique perspective in understanding the specific challenges faced by financial sector participants covered by their oversight and subject to their examination activities. Importantly, by having dedicated technology and innovation units resourced and led, at the explicit direction of a director/ senior leadership to engage in outreach, assessment, and testing (both in "beta" and "in-market") of new technological applications, companies shall benefit from the practical feedback and impact to specific regulatory issues for which covered institutions can/would be examined. In this way, such testing and practical deployment can be managed in the context of regulatory requirements vs outside of their purview or merely in response or avoidance of the same.
    - Furthermore, as existing or newly regulated institutions adopt new technology processes, such centers would be the natural place for those institutions to effectively time and coordinate the management of parallel processes in coordination with their functional regulators to ensure essential safety/soundness measures, redundancy practices and other risks are taken into consideration as new technology is rolled into live market production, and while others are ceased. This process would give tremendous comfort to new market entrants, non-traditional financial services companies – in particular nonbank FIs and fintech companies – as they look to participate in what is otherwise interpreted by many as a 'gotcha-oriented' financial regulatory environment. We are not necessarily offering or suggesting that such efforts should come with guaranteed safe-

harbor or immunity measures, but instead an affirmation that such efforts do not put undue or unknown regulatory risks on financial market participants—traditional and non-traditional.

- Enhancing Coordination/Engagement with Field Examiners:
  - Regulators should consider ensuring appropriate engagement within these centers by their field examiners. There is ongoing reluctance on the part of financial market participants and technology companies of revealing new capabilities to regulators for fear that examiners will remain steadfast to oversight and audit that serve to discourage or dismiss innovative processes or applications. Regardless of the many proactive outreach efforts by new market entrants (e.g. non-banks and fintech companies to federal financial regulators), too often there remains a disconnect between well-intentioned sector participants in bringing new technologies and methodologies to market – both within their own enterprises and as solutions to regulated financial institutions—and uninformed field examiners have often approached their work in *a tick-the-box* fashion for assessing regulatory adherence. This has served to significantly cool outreach by fintech and regtech companies, even when their commercial solutions can serve to benefit banks and other regulated financial institutions to better carry out their AML obligations more cost effectively and in keeping with the spirit of the BSA. Importantly, many solutions have benefits of application to AML/CFT among non-traditional/non-bank entities, whose activities to date fall outside the purview of federal regulators.
  - Reinforcing that there is senior leadership dedication to innovation and new technology applications would create an additional linkage between Washington DC-based policy makers and regulators with field examiners, such that their audit and review of covered institutions take into consideration measured approaches to meet AML/CFT obligations in robust ways. We would recommend that an explicit goal of senior leadership charged with management and oversight with these centers engage field examiners in the process of assessment, review and deployment of these new technologies in advancement of AML/CFT and other oversight goals.

- Enhancing Regional Efforts and State Coordination:
  - Increasingly, individual states are taking a lead, often through their individual Departments of Financial Services – or equivalent agencies – to liaise with industry by welcoming new technology innovation and coordination with financial industry participants. These efforts, while very welcome in particular to bank and non-bank financial institutions domiciled in those respective states, many find themselves potentially engaging in otherwise welcome testing and deployment of new reg-tech or fintech applications at the State level, but potentially running afoul or at cross-purposes with federal regulatory requirements. The simple reality that nonbank financial institutions, such as many money service businesses and money transfer operators (MSBs/MTOs), fintech companies, digital asset exchanges and others in the growing crypto-currency sector must ensure individual state-by-state registration in tandem with potential US federal oversight from one or more of the aforementioned regulatory agencies can be both commercially and regulatory burdensome.
  - Further, ongoing legal challenges between individual states and one or more federal regulators has served to exacerbate these challenges for companies working diligently to ensure regulatory compliance but could potentially be reinforcing processes that may be in conflict between one or more State or Federal agency regulations. We would

encourage that established innovation and technology centers provide for regional and state-to-state coordination as new market participants would be able to approach these efforts with similar good faith cooperation with both state and federal-level authorities in tandem. As such, we encourage that these centers be staffed and driven by regional sub-heads or similarly constructed senior leadership that would include regulatory professionals outside of Washington DC. Ensuring augmented staffing at each regulatory agency comes with appropriate senior level assignments and power will further reinforce their ability to speak with appropriate authority in representation of their respective agency's position and in furtherance of overall US policy goals.

- Strengthening Coordination By and Between Regulatory Agencies:
  - Alongside individual agency-led technology and innovation units, we encourage by mandate that agencies work within existing frameworks including the Financial Stability Oversight Council (FSOC) and the Federal Financial Institutions Examinations Council (FFIEC) processes for sharing knowledge, practical applications of new technology and reporting of such activities to Congress on a regular and timely basis.
    - Prior to the formation of the FSOC, no single regulator had responsibility for monitoring and addressing overall risks to financial stability, which the US is comprised of a myriad of financial firms operating across multiple markets. The formation of this important council was to facilitate regulatory coordination and information sharing that can better inform financial services policy development, consolidate the supervision of nonbank financial companies in particular, regardless of their form, and designated systemic financial market utilities and systems.[1] These goals are not only noteworthy in terms of their practical utility, but the FSOC also helps streamline activities in the US finance and banking community amidst an already crowded and often confusing landscape of cross-functional state and federal regulators operating across jurisdictional authorities. As we continue to see the growth of financial intermediation activities undertaken by non-traditional institutions and non-bank financial services companies, the FSOC can and should be a consolidation of authorities and oversight, and importantly a coordination and information center that should govern assessment and reporting of innovation and new technology development and related deployment in the industry. The FSOC could very well be, in form and function, the go-to Council for companies providing new technology applications that impact essential financial services activities, including payment processing and settlement, AML/CFT compliance and other activities impacting safety, soundness and consumer protection. In addition, innovative non-bank and fintech efforts that drive greater financial access can and should be shared through the FSOC to address important development goals and rules including those

[1] https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc

related to community development finance and the Community Reinvestment Act (CRA) among others.

- The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by a number of the core federal financial regulators, including the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB). Importantly, in 2006, the State Liaison Committee (SLC) was added to the Council as a voting member, which brought to the Council representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS).[2] This Council too, can and should serve as a coordination center for the sharing of information and insights regarding technological innovation and applications into the financial services sector by both bank and non-bank entities alike. With ongoing confusion in non-bank and fintech circles as to the manner in which to consolidate outreach between state-based and federal regulators, reporting up and to the FFIEC of and by individual regulator-led innovation and technology centers will prove invaluable to the sector.

- Regular reporting by individual regulators to the FSOC and FFIEC of specific technology applications driven to specific AML/CFT compliance goals and BSA obligations, and/or the application of new technologies in the delivery of specific products and services (e.g. secure payments, alternative lending, mobile banking, etc.) would be essential for regulators to share knowledge and application of such technologies across the industry. Such efforts would also reinforce and aid in consistent oversight and examination mechanisms across multiple regulatory authorities—at both the federal and state levels—as well as help codify new rulemakings impacting industry as related to AML/CFT or other important areas.

It is important to note that these efforts must not be limited to their mere establishment by Congressional mandate. The seriousness of these efforts needs to be reinforced with adequate funding support, including the increase in staffing numbers and pay-level for individuals charged with managing these regulator-led innovation and technology centers. Ensuring equity of pay and support between regulators and equality of opportunity across regions in the US for innovation center activities will serve to limit internal regulatory arbitrage and facilitate the recruitment, management and retention of participating professionals, who will feel empowered to speak and act on behalf the agencies they represent. Such support shall also allow for industry participants to be incentivized to participate in targeted innovation efforts and the practical deployment of new technologies to modernize AML/CFT activities by both bank and non-bank financial institutions – including the increasing efforts by a number of smaller, community-oriented regional and sub-regional financial institutions to form value-added partnerships with fintech and regtech companies to remain competitive in an increasingly evolving financial services sector. As stated above, such efforts shall pay dividends to other important policy goals

[2] https://www.ffiec.gov/

supporting inclusion, community based finance, and building economic resilience – all of which directly contribute positively to our financial integrity and AML/CFT goals and consequently to our national security priorities.

Conclusion: Financial Inclusion as a Matter of National Security

I am hopeful that my recommendations offered above will assist the Committee in considering further ways to strengthen this proposed legislation and drive greater public-private sector cooperation – in particular as it relates to innovation and the testing and deployment of technology to strengthen and modernize AML/CFT efforts and importantly drive financial inclusion. More importantly, I am hopeful that my testimony will help address the doubts and concerns that have prevented prior Congresses from adopting similar legislation in the past.

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 we have brought to driving financial inclusion vs 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, strengthen 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 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 foundation; extending this to the 25+% of the country's financially underserved and excluded—and ultimately to the 2.5-3B people globally underserved/excluded—ultimately serves to drive overall financial system integrity and security moving forward, but also underpins our collective national security at home and abroad.