Brick & Mortar to Bits & Bytes: Adapting the U.S. AML/CFT Regime for Digital Identity

Bank Secrecy Act Advisory Group (BSAAG)
FinTech/RegTech Working Group
Digital ID/eKYC Workstream[1]

Table of Contents

The Financial Action Task Force (FATF) *Guidance on Digital Identity* (FATF Guidance) envisions "Digital ID systems" as using "electronic means to assert and prove a person's official identity online (digital) and/or in-person environments at various assurance levels."[2] However, the FATF Guidance acknowledges that "[n]ot all elements of a digital ID system are necessarily digital. Some elements of the identity proofing and enrolment component can be either digital or physical (documentary), or a combination, but binding, credentialing, and authentication … must be digital."[3] Written for a broad audience of government authorities, regulated entities, and digital ID service providers from jurisdictions of varying political realities and stages of development in their Anti-Money Laundering (AML)/Counter Financing of Terrorism (CFT) regimes, the FATF Guidance's primary focus is primarily on true, end-to-end national digital ID systems.[4]

The reality is that most financial institutions[5] currently inhabit, and will likely continue to inhabit, a world straddling the paper and plastic identification of the past and the aspirations of end-to-end digital identification systems that the FATF envisions. The range of practices used to satisfy Bank Secrecy Act (BSA) obligations in the U.S. vary widely among online banks or neobanks, fintechs, and traditional financial institutions. But overarching the financial industry and its business models is the reality that there is deep political and cultural skepticism of, or even hostility to, a national ID system in the U.S.

Therefore, this Working Group (Group) acknowledges the likelihood that a fully realized national digital ID system will face unique political challenges and structural hurdles in the U.S.

---

[1] This draft whitepaper was drafted for review and presentation at the May 2021 BSAAG meeting. The views expressed in this document are those of the Workstream as contributed and agreed by workstream members, and not those of their employers.

[2] FATF, *Guidance on Digital Identity* ¶57 (Mar. 2020).

[3] *Id.* at ¶59 (emphasis added).

[4] *Id.* at ¶58.

[5] For purposes of this paper, "financial institution" encompasses those businesses identified in 31 CFR 1010.100(t), including banks, broker-dealers, money service businesses, casinos, and mutual funds, among others.

that it would not in many other countries[6] and that the financial industry will likely be living in that interstitial state of paper, plastic (i.e., "analog"), and "digital ID" for the foreseeable future. "Digital ID" in the U.S. will more likely evolve to include a mosaic of tools and services offered through Federal and State governments, digital ID vendors, credit ratings agencies and other data providers, and financial institutions themselves. As the mosaic evolves and financial institutions face continued commercial pressure to provide their customers with the kind of seamless online services they are already accustomed to in other service sectors (and countries), financial institutions will only increasingly identify and verify their customers through digital means, but with AML legal and regulatory requirements that were designed for analog identification processes undertaken by financial institution in their brick-and-mortar, not online, forms.

In this context then and utilizing FATF's terminology, this paper takes the functional view that "digital identity" or "digital ID" refers simply to:

> *electronic means [that can be used] to assert and prove a person's official identity online (digital) and/or [within] in-person environments at various assurance levels."*
>
> – FATF Guidance at ¶57.

This formulation acknowledges the realities of interstitial state between analog and digital identification our "mosaic" but allows us to chart a course for U.S. financial institutions who must continue to engage their customers in an increasingly digital world. It also encourages U.S. financial institutions to engage a key recommendation of the FATF Guidance to utilize the "anti-fraud and cyber security processes" already in common use by U.S. financial institutions, such as geolocation, IP addresses, and biometrics,[7] "to support digital identity proofing and/or authentication for AML/CFT efforts (customer identification/verification at on-boarding and

---

[6] For example, Singapore's myInfo/SingPass, Estonia's national ID-cards, or India 's Aadhaar number are all national, federated digital ID systems that may be used for CDD and digital onboarding. Others, like Sweden's BankID have sanctioned specific digital identity services for financial services onboarding.

[7] The FATF defines three distinct types of "biometrics":

- biophysical biometrics: attributes, such as fingerprints, iris patterns, voiceprints, and facial recognition—all of which are static
- biomechanical biometrics: attributes, such as keystroke mechanics, are the product of unique interactions of an individual's muscles, skeletal system, and nervous system.
- behavioural biometric patterns: attributes, based on the new computational social science discipline of social physics, consist of an individual's various patterns of movement and usage in geospatial temporal data streams, and include, e.g., an individual's email or text message patterns, file access log, mobile phone usage, and geolocation patterns.

FATF Guidance at ¶57.

ongoing due diligence and transaction monitoring)" even absent end-to-end, state-sponsored or authorized digital identity systems.[8]

B. Objectives

First, the U.S. AML regime should create the conditions for digital ID practices to take root in the U.S. financial industry by expanding and updating the existing customer identification program (CIP) rules for the different types of BSA-regulated institutions.[9] The current CIP Rules are nearly 20 years old, were primarily designed for in-person identification in brick-and-mortar branches, and are now quickly being dated by intervening advances in technology—smartphones, biometrics, artificial intelligence, etc. While the CIP Rules wisely preserved some flexibility, they still do not provide financial institutions sufficient regulatory certainty or the permission necessary to ensure digital ID elements can be included effectively in CIP and Know-Your-Customer (KYC) processes, especially in the way that the FATF is now advocating. Therefore, this paper recommends specific regulatory action, particularly in the CIP Rules, and interpretation that can begin to create the conditions and flexibility under which financial institutions may fully utilize digital ID's benefits, while mitigating its potential risks and better combating money laundering, terrorist financing, weapons proliferation, and other illicit transactions. For instance, the paper suggests revisiting the presumption in the CIP Rules that online identification and verification is inherently riskier, the requirement for banks to obtain the full nine digits of the Social Security Number (SSN), enhancing examiner guidance on new digital identification elements, and exploring usage of alternative identifying numbers, such as driver's license numbers as mobile driver's license (mDL) and state identification ecosystems mature and provide higher levels of assurance.

Second, the U.S. AML regime should incorporate more "optionality"—i.e., having more options, but not necessarily obligations—into CIP and customer due diligence (CDD) processes. Greater optionality would allow financial institutions to utilize the variety of "digital signals" inherent in a predominantly digital customer relationship—e.g., IP addresses, geolocation, biometrics, etc.—to contribute to a financial institution's understanding of its customer for KYC purposes. In their optionality, greater utilization of digital signals would not be mandatory for financial institutions—those able to manage their AML/CFT risks with traditional CIP and KYC processes would be able to satisfy their regulatory obligations without incorporating or relying on digital signals. However, financial institutions with digital relationships would be able to incorporate and rely on those signals in addition to or in lieu of some traditional KYC elements. As discussed in more depth in section II.D, this could include substituting the traditionally required

---

[8] *Id.* at Glossary, p. 101.

[9] See 31 CFR 1020.220 (banks); 31 CFR 1023.220 (broker-dealers); 31 CFR 1024.220 (mutual funds); 31 CFR §1026.220 (futures commission merchants and introducing brokers) (together, the CIP Rules). Other BSA-regulated financial institutions, including casinos/card clubs, money service businesses, insurance companies, dealers in precious metals/stones/jewels, credit card systems, loan or finance companies, and housing government sponsored enterprises, do not have a customer identification program requirement; however, they may have requirements to either identify a customer or verify a customer's identity for certain transactions.

CIP elements of Social Security Number (SSN) and address, either with sufficient assurance levels obtained with other digital elements or at lower risk levels, especially when considering financial inclusion policy rationales.

Third, financial institutions and regulators should continue to define the benefits of and rationales for digital identity, but especially its potential to both enhance the effectiveness of AML

> ***[o]fficial identity that can change over time as the identified individual develops a progressively more robust digital footprint that provides an increasing number of attributes and/or authenticators that can be verified against an increasing number and range of sources.***
>
> – FATF Guidance at p. 104.

compliance and increase financial inclusion.

Fourth, this paper seeks to expand on the concept of "progressive identity" explored in the FATF Guidance. As defined by the FATF, "progressive identity" is an:

Progressive identity recognizes that digital ID is not simply a new method for static identification and verification, but can facilitate the "customer journey" through which customers increase their digital footprint and traditionally underrepresented customers can seek more and varied services as they develop a more robust digital footprint with a financial institution, all while providing financial institutions tools that could be used to better understand the nature and purpose of the customer relationship. By utilizing progressive assurance levels, financial institutions should be able to able offer limited, lower-risk products and services for customers in the initial steps of that "journey" relying on simplified due diligence frameworks already sanctioned by FATF, only requiring enhanced assurance if customers wish to increase the depth and complexity of their relationships with the financial institution.

These approaches to digital ID have potentially profound policy implications and benefits. Expanding CIP elements could enhance the security of our identification ecosystem by reducing reliance on the already highly compromised SSN. Progressive identity would help financial institutions address financial inclusion, allowing and encouraging them to take on customers they have in the past overlooked or who themselves have been deterred from even seeking services from financial institutions (and make that onboarding process easier for the customer), while also focusing financial institutions on behavioral risk rather than cruder risk proxies like geography or product type. Focusing on behavioral customer risk and leveraging the digital signals that many financial institutions are already using for their fraud and cyber-security processes to mitigate operational risk would allow financial institutions to refocus the massive human resources currently allocated to KYC and train them on more effective techniques for proactively detecting financial crime.

dealers, and other financial institutions" through "the mail, electronically, or in other situations where the accountholder is not physically present at the financial institution".[12] Those numbers have only grown since 2001 for mutual funds and broker-dealers, but also for banks for whom it was less customary to open accounts remotely in 2001. This concern led in part to the flexibility built into particularly the non-documentary verification option of the CIP Rules and informed the credit card exemption,[13] which explicitly granted banks the ability to obtain identifying information from third-party sources prior to extending credit in large part because the credit card banks' business model entailed opening accounts remotely by telephone or at third-party points of sale.[14] Just as credit card banks' business model in 2003 was predicated on remote, non-face-to-face onboarding, many financial institutions have had their business models disrupted by technology and are now heavily reliant on their ability to conduct non-face-to-face onboarding through smartphones and other electronic devices.

B. Clarify that that non-face-to-face identification is not always inherently riskier than face-to-face identification

The language of CIP Rules suggest that a customer opening an "account without appearing in person" is a "circumstance[] that increases the risk that the financial institution will be unable to verify the true identity of a customer through documents."[15] That presumption, and its reflection in the FFIEC's BSA/AML Manual[16] (FFIEC Manual), should be reassessed in light of the FATF's observation that non-face-to-face identification "may be standard risk, and may even be lower risk,"[17] the MOBILE Act's Congressional sanction of digitally transmitted ID documentation, the current verification practices for many financial institutions operating online, and the state of the technology itself that has evolved well beyond what was available in 2003 when the CIP rule was promulgated.

---

[12] H.R. Rep. No. 107-250, pt. 1, at 63 (2001) (discussing the Financial Anti-Terrorism Act of 2001, which was later consolidated in the USA PATRIOT Act).

[13] 31 CFR §1020.220(a)(2)(i)(C) ("In connection with a customer who opens a credit card account, a bank may obtain the identifying information about a customer required under paragraph (a)(2)(i)(A) by acquiring it from a third-party source prior to extending credit to the customer").

[14] Final Rule, *Customer Identification Programs for Banks, et al.,* 68 FR 25089, 25097 (2003) (citing H.R. Rep. No. 107-250).

[15] 31 CFR §1020.220(a)(2)(ii)(B)(2) (bank); 31 CFR §1023.220(a)(2)(ii)(B)(2) (broker-dealers); 31 CFR 1024.220(a)(2)(ii)(B)(2) (mutual funds); 31 CFR §1026.220(a)(2)(ii)(B)(2) (futures commission merchants and introducing brokers).

[16] Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual,* Customer Identification Program at 5 (2021).

[17] FATF Guidance at ¶3; *see also* id. at ¶25 ("If, as a matter of internal policy or practice, non-face-to-face business relationships or transactions are always classified as high-risk, [regulated entities should] consider reviewing and revising those policies to take into account that customer identification/verification measures that rely on reliable, independent digital ID systems, with appropriate risk-mitigation measures in place, may be standard risk, and may even be lower-risk").

Where in 2003 a financial institution might have only the identification documentation and their impressions of an in-person account opening, it now may have more identification and verification data points from a customer relationship initiated online than in-person. In addition to non-documentary verification methods contemplated at the time of the CIP Rules' adoption, facial recognition techniques can now compare the government-issued photo ID document with real-time video calls or video-selfies, effectively replacing human vision with a computer's and establishing confidence that the individual behind the device during onboarding is in fact the onboarded personality.[18] In real-time, financial institutions are now capable of: verifying that the information provided by the prospective customer matches the government-issued photo ID document scanned by the device; validating the authenticity of the document and device via third-party software and mobile applications; and confirming that the photo on the document matches the individual's facial biometric as presented through the device which can be recorded in the customer's KYC file.

Though the ID document may be transmitted digitally and the account opening conducted "without appearing in person," today's remote digital verification of ID documents may in fact pose fewer risks than an in-person identification and verification that does not also use these techniques. The use of the biometric checks and specially trained screeners for inconclusive digital results adds an additional layer of protection against stolen IDs and impersonation attacks that can meet or exceed the reliability of traditional face-to-face verification. Even setting aside the potential foibles of human judgment in an in-person visual identification, an online onboarding simply captures more data by which to understand the customer, such as email address, device information, IP address, and geo-location, and allows the financial institution to cross-reference those data points to existing databases and form a more holistic view of the customer.

As larger scale reform for the CIP Rules is worked through, regulators could also address this point for examiners in the FFIEC Manual and/or for financial institutions through FAQs clarifying that the CIP Rules' presumption here is limited to situations where, at the time the rules were crafted, there would have been no reliable way to digitally convey documentary identification such as a driver's license and acknowledge that, today, there are viable and secure ways to convey and verify that documentation remotely.

C. In the near-term, explicitly permit banks and other financial institutions to collect the "last-four" of the SSN with adequate verification and retention of the "full-nine"

Truncation of the SSN has become a standard information security practice in different areas of society.[19] However, the bank CIP Rule alone explicitly requires that the four elements of

[18] Importantly and as discussed below, we must be critical of and continue to assess and improve technologies like facial recognition, which have thus far proven less effective at recognizing, for instance, darker skin tones.

[19] *See, e.g.*, Internal Revenue Service, *Use of Truncated Taxpayer Identification Numbers on Forms W-2, Wage and Tax Statement, Furnished to Employees,* 84 F.R. 31717 (2019) (permitting employers to print only the last four

II. Modernize the CIP Rules to Adapt to Evolving Digital Identification Practices

As public and private stakeholders provide new tools for digital identification and verification, the U.S. AML regime should be prepared to ingest them and acknowledge the changed landscape and expectations of cybersecurity.

A. The Customer Identification Program rules were built to last and adapt but were still created primarily for brick-and-mortar relationships.

The different iterations of the BSA's CIP Rules provide inherent flexibility, both in their fundamental requirement simply to have procedures that "enable [the formation of] a reasonable belief that [the financial institution] knows the true identity of each customer" and the ability to obtain "documentary" or "non-documentary" verification—itself a version of the "optionality" concept that this paper advocates expanding. The rules do not absolutely require the presentation of government-issued identification, mandate in-person presentation of documentation, or even require an identification photograph.[10]

For example, the CIP Rules arguably provide sufficient flexibility for the growing practice of accepting a digitized transmission of a driver's license, which is further supported by 2018's MOBILE Act.[11] That Act allows financial institutions to accept and record information from a scanned driver's license or personal identification card to verify the authenticity of the identification and the identity of an individual requesting to open an account or obtain a financial product or service. However, other aspects of the CIP Rules, such as requiring banks to collect identification data "from the customer" or the apparent presumption that non-face-to-face identification is inherently riskier than in-person identification, undermine some of that flexibility. These limitations are inconsistent with the MOBILE Act's intent to encourage the digital delivery of financial services to address increasing mobility and lack of fixed addresses in the population, consumer expectations for digital products and services, and the unfortunate reality that face-to-face identification requirements also may raise health and safety risks as during the COVID-19 pandemic.

Though the CIP Rules were prescient in utilizing both documentary and non-documentary verification methods, it is worth considering whether they can be updated or clarified to reflect the reality that online relationships and the technologies that manage those relationships have only become more prevalent across all BSA-regulated financial institution types and forced many to rely increasingly on non-documentary identification and verification. Even in 2001, Congress recognized that the fact that "[m]illions of Americans open accounts at mutual funds, broker-

[10] See, e.g., 31 CFR 1020.220 ("documents may include... [f]or an individual, an unexpired government-issued identification").

[11] The Making Online Banking Initiation Legal and Easy [MOBILE] Act (enacted as Section 213 of the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018).

CIP, including the SSN, be collected "from the customer," which banks and their examiners commonly read as collecting the full-nine digits directly "from the customer." Though this requirement is only explicitly present in the bank CIP Rule, this group understands anecdotally that other financial institutions commonly understand it to be a requirement in their respective industries.[20] In any event, however, it is now common practice for some traditional financial institutions and certainly for fintechs typically regulated as MSBs to collect only the "last four" digits of the TIN/SSN "from the customer" when establishing a business relationship online and then verify and/or collect the remainder from a credit rating agency or other authorized third-party that can match the customer to the partial TIN/SSN (in which case, the full-nine digit SSN is never transmitted). Allowing the collection of the last-four digits of the SSN, which are its most unique numbers, while ensuring collection of the full- nine from a third party would comport not only with better information security practices, but also with consumer expectations and wariness in using the SSN at all.

Even though obtaining the last-four digits is still susceptible to identity theft because SSNs are so widely available and because the last-four digits are the most unique, the use of the last-four digits reduces the data security and privacy risks in acquiring and transmitting the full-nine digits. As a matter of industry practice, many financial institutions that collect the full-nine digits now send them to a credit reporting agency for verification purposes in any event. Sending only the last-four digits would therefore reduce data security and privacy risks while also being sufficient in most circumstances for identification and verification purposes—utilizing valid name, address, date of birth, and verifying the last-four digits against the full-nine presents low risk of misidentification. Banks or other financial institutions who may still collect the full-nine will also need to consider any other potential risks in larger scale adoption of last-four and establish clear guardrails for requiring the full-nine where a last-four method has failed. Fortunately, there is already a wealth of best practices and techniques from the large number of other financial institutions and vendors that have utilized these practices for some time already. Perhaps more important than the identity theft, data security, and privacy risks, is the possibility that requiring the full-nine in an online setting will likely discourage potential customers from opening bank accounts online because widely accepted and promoted data security practices suggest that provide the last-four whenever possible.[21] Utilizing last-four would also have the knock-on effect

---

digits of the SSN on W-2 statements and noting the ability to identify individuals with last-four together with name and address).

[20] While the bank CIP Rule specifies that the four CIP elements must be collected "from *the* customer", all the CIP Rules require their covered FIs' CIP contain procedures that specify what identifying information must be obtained "from each customer", followed in close proximity by the four CIP elements. This proximity may have led to a reading that the four element themselves must be "obtained from each customer." The non-bank CIP Rules, however, only require the CIP to determine which elements must be collected "from each customer", not that each element must be collected "from the customer," and therefore may be more susceptible to clarification by FAQ.

[21] *See, e.g.*, Federal Trade Commission, *What to Know About Identity Theft* (suggesting consumers ask if they can only provide the last-four digits when asked for their SSN); American Association of Retired Persons, *Guard Your*

of streamlining collection of CIP information from beneficial owners and especially from corporate controls persons, who are sometimes reluctant to potentially compromise their own identity in service of their employer.

The OCC's recent Interpretive Letter 1175,[22] permitting the requesting bank to use the last-four digits in a specific circumstance, may pave the way by confirming that "collecting partial TINs from customers does not present any additional risk of money laundering since [the requestor's operating subsidiary] will obtain the full TIN from a reliable third party source that will enable it to form a reasonable belief that it knows the true identify of its customer." Though the Interpretive Letter is limited to the facts presented by the requestor, its rationale should be more broadly accepted, if not encouraged, across the financial industry.

Wide-scale adoption of last-four may also be a relatively easy regulatory change to make outside of full-scale revision of the CIP Rules. First, regulators could issue a Frequently Asked Question (FAQ) clarifying that a customer providing their last-four digits and consent to collect their full-nine digits from an authorized third party is the equivalent of obtaining the full-nine digits directly "from the customer." Second, the "from the customer" language may be susceptible to carve out from the CIP Rules' exemptive relief provisions. Since the practice of collecting full-nine originates with the "from the customer" language of the Bank CIP Rule alone, it would not require a regulatory and AML risk analysis for all BSA-covered financial institutions. Third, the CIP Rule's exemptive relief provision authorizes the "appropriate Federal functional regulator, with the concurrence of the [Treasury] Secretary" to "exempt any bank or type of account from the requirements of this section" by simple order, provided that exemption is consistent with the purposes of the BSA, safe and sound banking, and other appropriate factors.[23] Though the credit card exemption was written into the regulation itself, the logic of its flexibility to account for the nuances of the commercial context and privacy expectations of customers at the time may also provide a guidepost for the rationale for a last-four exemption.

D. Look beyond the CIP Rules' "Core Four" as identifiers

The only identification elements that the USA PATRIOT Act (in amending the BSA) explicitly required for the identification and verification of accountholders were name and address[24]—it did not explicitly mandate collecting or maintaining the SSN or date of birth. The USA PATRIOT Act also required the Secretary of the Treasury to "take into consideration the various types of accounts maintained by various types of financial institutions, the various methods of opening

---

Social Security Number (suggesting the protection of even the last-four by asking if a company can accept an alternative identifier).

[22] Office of the Comptroller of the Currency, *Interpretive Letter #1175 re: Customer Identification Program Rule Exemption Request* (Nov. 16, 2020, published Dec. 2020).

[23] 31 CFR §1020.220(b).

[24] 31 U.S.C. §5318(l)(2)(B) ("maintaining records of the information used to verify a person's identity, including name, address, and other identifying information").

accounts, and the various types of identifying information available."[25] Since there are now many more methods of opening accounts and types of identifying information available than there were in 2001 at the time of the USA PATRIOT Act's passage and the implementing regulations for the CIP requirement in 2003, and the Anti-Money Laundering Act of 2020[26] (AML Act) is causing a broader reconsideration of the U.S. AML regime, this is an appropriate inflection point for Treasury to reconsider its CIP Rules. Assuming, however, that "name" is a fundamental requirement for identification and as a practical matter "date of birth" (or at least month and year of birth) may be a necessary identification element for OFAC screening purposes and possibly ensuring true matches in 314a or 314b requests, we should at least reconsider the SSN and address as absolutely required CIP elements and assess potential alternatives at this moment in the evolution of the BSA/AML regime. As discussed in more depth below, reconsidering whether alternative identification elements could substitute for identifying number and address could have important implications for the ability of financial institutions to utilize digital identity systems at the state level and address increasing concerns over financial inclusion for those who may lack fixed addresses or SSNs.

In addition, we should clarify and distinguish that identifiers may and sometimes should be different than the record-keeping requirements for customers. For instance, even if the SSN is not required as an identifier it is sometimes required for other regulatory purposes, such as tax reporting, and is often a helpful data point for law enforcement. Financial institutions could, however, still collect the SSN from credit reporting agencies for regulatory, tax, and record-keeping purposes, as well as assisting law enforcement.

1. Reduce the dependence on the SSN as an identifier and open the door to alternative identifying numbers

The deficiencies of the SSN from an identification, verification, authentication, and general cybersecurity perspective are well-documented. Requiring a new customer to provide an SSN in 2003 was much more valuable in authenticating that the customer was who s/he claimed to be because knowledge of one's SSN was generally more private then and the numbers themselves had not been compromised the way many of them have been today.[27] Today, however, after so many large-scale data breaches and ready accessibility of SSNs from illicit brokers, the SSN is no longer as valuable particularly as an authenticator and, as discussed above, customers are increasingly wary of sharing it. Moving away from it as a required element of CIP and allowing other identification numbers in its place as long as they provide financial institutions that "reasonable belief" in the "true identity" of their customers would likely be beneficial not only for financial institutions' identification purposes and fraud reduction, but also for customer privacy,

---

[25] *Id.*

[26] AML Act of 2020, H.R. 6395 (2021).

[27] *See, e.g.*, The Better Identity Coalition, *Better Identity in America: A Blueprint for Policymakers* (July 2018) (advocating the cessation of using the SSN as an authenticator and limiting its use as an identifier).

information security, financial inclusion, and the health of the country's identity ecosystem.[28] Moreover, as discussed below, the Anti-Money Laundering Act of 2020 allows for the use of other potential identifying numbers in identifying beneficial owners of legal entities and even creates a new form of identifier to be issued by FinCEN, both of which may expand the identification landscape to broader sets of identifying numbers.

As the most common documentary identification and verification source for natural persons, driver's licenses and state-issued identification and their identification numbers are the prime candidate for expanding the "optionality" for identification number. Driver's license and state identification card numbers are themselves readily verifiable with credit ratings agencies and other providers, just as SSNs are. The widespread adoption of the more reliable REAL ID standard for driver's licenses and identification cards, which requires a thorough verification of the "Core Four" including the SSN itself by state government issuers,[29] will also make driver's licenses and identification card numbers more reliable identifiers generally. In addition, state mobile driver's licenses (mDLs) may be showing the most promise and progress as end-to-end digital identification systems—and may ultimately get more traction with a general public that has viewed Federal identification systems with skepticism and suspicion since the advent of the SSN itself.[30]

Apple has been actively advancing the possibility of greater adoption and consistency of mDLs by announcing in June 2021 that iOS 15 would allow customers in participating states to add their drivers licenses or state IDs to its Wallet App.[31] More recently, Apple has announced the initial wave of participating states and that the Transportation Security Administration (TSA) will enable their use at certain airport checkpoints.[32] While Apple has promised privacy, concerns about the issue and potential inconsistencies across states and by government actors may

---

[28] National Institute of Standards and Technology, *Special Publication 800-63A Digital Identity Guidelines* §8.1.1 (June 2017) (noting that "[o]verreliance on the SSN can contribute to misuse and place the applicant at risk of harm, such as through identity theft", that "operational necessity" for use of the SSN can only be demonstrated by an inability to alter systems, processes, or forms due to cost or unacceptable levels of risk", and the federal agencies are required to "review any decision to collect SSN relative to their *obligation to reduce the collection and unnecessary us of the SSN as necessary*") (emphasis added).

[29] In this sense, REAL ID driver's licenses will essentially become derivative of SSN-based identification. However, to the extent that it may be carried out at more stringent assurance levels by state government actors, REAL IDs may help limit the use of the SSN in private-sector relationships.

[30] *See, e.g.*, Thales Group, *Digital Driver's license-your ID in your smartphone* (detailing pilots in Idaho, Colorado, Maryland, and Washington, DC); Idemia & Arizona Department of Motor Vehicles, Treasury Department Virtual Policy Forum, *Spotlight Session: Mobile Driver's Licenses* (Feb. 2021).

[31] Apple Inc., *Press Release: iOS 15 brings new ways to stay connected and powerful features* (June 7, 2021);

[32] Apple Inc., *Press Release: Apple announces first states signed up to adopt driver's licenses and state IDs in Apple Wallet* (Sept. 1, 2021) (announcing Arizona, Connecticut, Georgia, Iowa, Kentucky, Maryland, Oklahoma, and Utah as among the first states to allow their mDLs in Apple Wallet).

"acceptable identification documents," while collecting the TIN for recordkeeping purposes from third-party services and eventually via APIs with the government issuing authorities.

To further promote financial inclusion, financial institutions, regulators, and law enforcement should also consider whether alternative identifying numbers could be used at lower assurance levels for correspondingly lower dollar, limited service accounts even without a record-keeping requirement for an SSN.[36] As discussed in more depth below, in digital or predominantly digital relationships, the digital signals from a customer that a financial institution collects during the customer lifecycle may themselves add to the level of identity assurance over time, or conversely, customer account activity and/or additional product usage may trigger the need for increased assurances. In addition to promoting financial inclusion and equity, such an approach could increase "SSN-shy" customers' access to financial services instead of use of less transparent, informal value transfer systems, which could benefit law enforcement.

2. Expand the Scope of the BSA's Requirement for "Address"

Though "address," unlike "identification number," is specifically mentioned in the BSA as an identification element, it has a history of broader interpretation than the "residential or business street address" required by the CIP Rules. The CIP Rules themselves make allowances for individuals without fixed residential or business addresses to provide Army or Fleet P.O. boxes or the residential or business address of a "next of kin or of another contact individual."[37] In 2004, FinCEN issued an FAQ indicating that rural route numbers are acceptable as addresses and that in the absence of such a number or address for next of kin or another contact individual, even a "description of the customer's physical location" would suffice.[38] Similarly, in 2010, FinCEN issued a ruling on the CIP requirements allowing victims of domestic violence in state-sponsored address confidentiality programs to use the P.O. boxes assigned by their state programs.[39] While this guidance is helpful, FinCEN could advance financial inclusion in both analog and digital identification by expanding upon the "next of kin or of another contact individual" option in the CIP Rules by utilizing the FATF's suggestion of allowing "trusted referees", including for example local government authorities, employers, or school administrators, to vouch for an applicant.[40] In the digital identity context, the National Institute of Standards and Technology (NIST) makes allowance for the use of trusted referees in its *Digital Identity Guidelines*, which provide digital ID

---

[36] For example, alternative identifiers may be needed to assist victims of human trafficking recover when their original identities have been compromised as a result of their victimization.

[37] *See, e.g.*, 31 CFR 1020.220(a)(2)(ii).

[38] FinCEN, *Guidance on Customer Identification Regulations—FAQs: Final CIP Rule* (Jan. 2004).

[39] FinCEN, *Ruling FIN-2009-R003: Customer Identification Program Rule - Address Confidentiality Programs* (Nov. 3, 2009).

[40] FATF Guidance at ¶¶169-71.

inevitably linger and remain a barrier to use.[33] There may also be drawbacks for verifying financial institutions such as the fact that drivers' licenses may be revoked or expire, or individuals may carry driver's licenses from multiple states. The fact that physical driver's licenses are easily stolen and presented in full in a variety of settings, could make their identification numbers more vulnerable to fraud and identity theft.

While these are certainly concerns, there may also be advantages to mDLs that protect them from some of these potential weaknesses. If an iPhone is stolen or lost, bad actors will have a much more difficult time extracting mDL information from the iPhone than the face of a plastic license. mDL proponents, including Apple, tout the possibility of a "Privacy View", limiting access to those information elements required by the verifying requestor, confirming for example to a liquor store only that the bearer is over 21 without revealing even their birth date, identification number, or any other identifying information while revealing more to a TSA or law enforcement officer.[34] Most tantalizingly, perhaps, mDLs offer a clear path to linking verification systems directly to state agencies as official, authoritative "sources of truth" for identity—the end-to-end digital ID system. The decentralized and dispersed efforts of different states as our "laboratories of democracy" may even be a strength in this context. While Apple's early efforts are currently limited to proving identity in the physical world to law enforcement and the TSA, their broader adoption and potential linkages to DMVs and other state sources as verifiers make them strong candidates both for greater use and inclusion in the mosaic of our digital identity ecosystem, proving identity online, and for use of their identifying numbers by financial institutions for CIP purposes. In time, financial institutions and third-party identity providers should be able to establish Application Programming Interfaces (APIs) with DMVs and state identification providers directly, or even blockchain authenticated identity tokens.

The Corporate Transparency Act (CTA), as part of the AML Act, has also recently opened the door for alternatives to the SSN by not requiring the provision of an SSN for beneficial owners but rather only a "unique identifying number from an acceptable identification document," and indicating that the "acceptable identification document" may be a nonexpired driver's license, state identification card, or domestic or foreign passport.[35] Opening the door even a little more, perhaps, the CTA also authorized the use of a unique "FinCEN identifier," which the agency will be required to issue to both entities and individuals that otherwise provide the required identifying information. While much remains to be determined with respect to the CTA, the CIP Rules' requirement to collect Taxpayer Identification Number (TIN) (i.e., SSN for individuals and EIN for legal entities) for identification and verification purposes should be opened up to a risk-based approach that would allow for the collection of other "unique identifying numbers" from

---

[33] *See, e.g.,* American Civil Liberties Union, *Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom* (citing possibilities of police access and tracking without adequate safeguards).

[34] *See*, Wash. Post, *Your driver's license could soon live on your phone. Here's what you should know.* (Oct. 11, 2021).

[35] Corporate Transparency Act (AML Act of 2020), H.R. 6395, Div. F, §6403 (2021).

assurance frameworks and standards in the U.S. and are widely considered authoritative elsewhere.[41]

While expansion of the "trusted referee" concept could enhance financial inclusion, the nature of digital identification and relationships themselves may provide even greater flexibility in banking those in underserved communities without a fixed residential or business address. Signals and data points available in a digital relationship may allow financial institutions to conduct the appropriate level of transaction monitoring for customers who are unable to provide a fixed address. For instance, a customer with no fixed address but an identified and authenticated electronic device bound at an acceptable assurance level who consents to geo-location may provide a better "description of the customer's physical location" than the potential uncertainties of locating that customer through "next of kin" or "another contact individual"—potentially allowing financial institutions to consider banking persons they might not have previously, even if at more restrictive, risk-based service levels. The FATF's 2017 supplement on CDD to its 2013 Guidance on financial inclusion acknowledges this possibility and the likelihood that the sustainability of financially inclusive business models may be dependent on leveraging technological solutions like these.[42] The intent behind requiring a physical address was to ensure that banks and law enforcement be able to locate a particular customer. Where digital identification information allows for a similar or perhaps even greater degree of certainty of customer location as physical address, it should be treated equivalently if not with greater certainty.

E. Ensure the CIP Rules' documentary verification examples and/or related examiner guidance are adaptable to a digital identification environment

The CIP Rules provide only one example for documentary verification of individual customers: "unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport."[43] While there is built-in optionality for financial institutions to take a risk-based approach as to acceptable identification documentation, the example could potentially be enhanced to accommodate changes in the way digital identity may be provided. As it stands, the example suggests

---

[41] NIST, *Special Publication 800-63A Digital Identity Guidelines* §5.3.4. Note that NIST issued a call for comment on its current guidelines in June 2020.

[42] FATF, *Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence* at 25 (2013, updated Nov. 2017) ("FATF Financial Inclusion Guidance") ("Increasingly, digital financial inclusion also includes the use of digital identity products and services to provide individuals with proof of identity for CDD purposes (though conventional and other alternative means of identifying customers and verifying identity may also be used). It also increasingly involves technological solutions used by financial institutions to fulfil their compliance obligations, for instance using big data collected through mobile phone usage, to monitor customers' transactions in a cost-effective manner. This is an important factor regarding the sustainability of the business models developed by financial institutions to reach out to low-income, unserved and underserved groups").

[43] *See, e.g.*, 31 CFR 1020.220(a)(2)(ii)(A)(2).

"government-issued" identification, when in many jurisdictions "government-authorized" digital identity service providers could potentially provide greater assurance levels in identification.[44] The flexibility built into "photograph or similar safeguard" is also helpful but, even in the context of physical identification, is now dated when "safeguards" may include a range of technical advances, including holograms, UV printing, microprinting, laser perforation, etc.[45] For advancing the acceptance of, and best practices for, digital identification, it may be helpful for the CIP Rules themselves, examiner guidance like the FFIEC manual, or FAQs to clarify that, while the photograph may still be the gold standard, the range of safeguards has expanded dramatically since the CIP Rules' issuance and that, in addition to photographic evidence, it may helpful to financial institutions to have reference to the new range of photographic tools (selfies, liveness, biometrics, e.g.) and assurance levels set forth by an authoritative standard setting body like NIST.

F. Ensure the CIP's rules' non-documentary verification element and/or related guidance for examiners are fit for a digital environment

While the CIP Rules' current examples for non-documentary verification have a helpful degree of flexibility, as discussed previously, they were crafted primarily for an analog identification environment and before many of the digital signals referenced above existed or were commonplace. Regulators should therefore also consider whether the CIP Rules' specification of non-documentary verification methods is sufficient for the digital identification environment. The current examples specified in the CIP mostly remain useful today: "contacting a customer; independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement." The "comparison of information" to "a consumer reporting agency, public database, or other source", in particular, is increasingly utilized over the other non-documentary and documentary verification methods in online customer relationships. However, additional examples that are both technology-neutral and principles-based could attune and encourage financial institutions and examiners to the possibilities of digital non-documentary verification. For instance, the rules could simply add a category that suggests "assessing data and assurance levels relevant to the delivery channel."

---

[44] *See, e.g.*, FATF Guidance at ¶55 ("Typically, proof of official identity has been provided by—or on behalf of—governments. In the digital era, we have begun to see new models, with digital credentials provided by, or in partnership with, the private sector being recognized by the government as official proof of identity in an online environment (e.g., NemID in Denmark), alongside more traditional government-issued digital credentials (e.g., electronic national IDs).").

[45] *See, e.g.*, Dep't of Homeland Sec., Request for Information: *Minimum Standards for Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Mobile Driver's Licenses*, 86 FR 20320, 20322 (Apr. 19, 2021) (distinguishing physical security features from electronic security features of mobile driver's licenses).

Though amending the CIP Rules would be the most effective way to ensure effective adaptation to digital identification, training examiners to consider a financial institution's usage of digital signals as a valid part of identifying, verifying, and even enhancing ongoing CDD obligations, as discussed below, would also be helpful. Accordingly, the FFIEC could consider amending the FFIEC Manual's CIP section to reflect even that the "comparison of information" element could include an assessment of assurance levels, particularly through digital signals that could impact onboarding, such as MAC/IP address, geolocation, email age, and website interaction. Although the FFIEC Manual's CIP section was only recently updated, the principles reflected here and in the FATF Guidance could also be reflected in the Manual's "Electronic Banking" (2014) section or even in a standalone section on AML in the FFIEC's booklet on E-Banking, which was issued in 2003. The utilization of some of these digital signals is, of course, also predicated on having access to them—if customers are unwilling to provide access to them either at onboarding or during the course of the customer relationship, customers could choose to be subject to more manual monitoring, KYC refreshes, and their attendant inconveniences. For their part, financial institutions may choose to assess the feasibility or risks of the relationship in those circumstances and limit them accordingly.

Case study in optionality to the north: Canada

FINTRAC's recent publication of guidance for Canadian financial institutions on identifying and verifying customers explicitly adopts an "optionality" approach that may be instructive for the U.S. FINTRAC offers five different ways to identify and verify a person, including the more recognizable government-issued photo identification and "credit file" method (i.e., utilizing a credit bureau similar to U.S. financial institutions). FINTRAC provides guidance for digitally provided government-issued photo ID, requiring that FIs have a process in place to authenticate the ID, and walking through examples of how this may be accomplished with digital photographs of the ID, selfies, and live video chat. However, FINTRAC also offers financial institutions a "dual process" method by performing any two of the following three elements:

1. refer to and confirm information from a reliable source that includes the person's name and address;
2. refer to and confirm information from a reliable source that includes the person's name and date of birth; or
3. refer to information that includes the person's name and confirms that they have a deposit account, a prepaid payment product account, or a credit card or other loan account with a financial entity, and confirm that information.

The information may come from "statements, letters, certificates, forms or other information sources" either in the original or in paper or digital copy. However, the sources of any two elements used may not be the same. The dual process method would allow a customer to obtain financial services who may both lack government-issued identification and a credit file, although a credit bureau may be used to prove on the two elements

by Congress in the passage of the AML Act of 2020,[49] and echoed by industry bodies like the Wolfsberg Group,[50] consultants and trade groups,[51] and thinktanks.[52] As the FATF suggests, encouraging and supporting digital identity systems and the effective use of digital identification techniques are exactly the kind of regulatory initiative that can allow financial institutions to refocus their AML/CFT programs on those more effective techniques. The effective use of digital identity in AML/CFT programs will not only allow the reallocation of cost savings, but itself will also produce more and more valuable information in the detection and prevention of ML/TF, as financial institutions leverage those digital signals that are increasingly defining their customer relationships. For example, one major investigative firm has related the effectiveness of utilizing digital signals and "following their data" by analyzing IP address data that revealed connections across a large number of purportedly unrelated customers, exposing a complex fraud and money laundering network. [53]

2. Digital Identity and Financial Inclusion

Though the FATF's March 2020 Guidance made a strong case for advancing financial inclusion particularly in developing countries by harnessing digital identity in AML/CFT programs, its authors likely could not have foreseen the outsized imperative financial inclusion would take in the ensuing year as governments even (perhaps especially) in developed economies like our own struggled to distribute funds at unprecedented speeds to the public to counteract the economic effects of the COVID-19 pandemic.[54] An effective system of digital identification not only would have hastened the stimulus and unemployment programs, but would also have helped the programs actually reach their intended recipients with less fraud and error.[55] Even more important, an effective digital identification system that fostered financial inclusion, could have helped the government reach more of those that have been most marginalized and vulnerable. As reported by *The New York Times* earlier this year, many homeless people lacking fixed addresses, identification, and resources were reportedly unable to receive the stimulus funds to which they

---

[49] *See* AML Act, §6002.

[50] Wolfsberg Group, *Statement on Effectiveness* (2019).

[51] *See, e.g.*, Deloitte & IIF, *The Global Framework for Fighting Financial Crime: Enhancing Effectiveness & Improving Outcomes* (2019).

[52] *See, e.g.*, RUSI, *Financial Crime 2.0*; Brookings Institution, *3 steps to improve anti-money laundering regulation* (2020).

[53] Tax Justice Network, *The role of banks and digitalised beneficial ownership registries* (July 2020) (describing analyses performed by Kroll in identifying the relationships of beneficial owners).

[54] *See* FATF Guidance at ¶109.

[55] *See* Center for Strategic & Int'l Studies, *The United States Has an Opportunity to Lead in Digital Development* (Mar. 30, 2021) (noting how "[t]he unforeseen devastation caused by the COVID-19 pandemic has highlighted the importance of digital payments and digital ID infrastructure for mitigating socioeconomic challenges" and citing the success of India's universal digital identification system—the Aadhaar—to effect cash transfers).

were entitled.[56] There are of course many more prosaic but still vitally important use cases for utilizing digital identity to ensure that more routine social safety net payments are made to their intended recipients safe from fraud and abuse.

The use of digital identification to reach underserved populations may not be a panacea, as there are well-known barriers to access to technology that will inevitably affect some in those populations.[57] Sometimes referred to as the "digital divide", lower income populations simply have less or less reliable access to the technologies that would facilitate digital identification. There is some reason for optimism on this front, however, as recent studies have found that 93% of the U.S. adult population use the internet, 97% use cell phones of some kind, and 85% use smart phones—and the percentages are regularly increasing.[58] In a potential silver lining, the pandemic laid bare the deficiencies of digital access particularly in education and concerted efforts by the government to facilitate access to underserved populations appear to be following.[59]

Case study in financial inclusion to the south: Mexico

Mexico has, since 2011, utilized a four-tier system of account opening at increasing risk levels to enhance financial inclusion:

- Tier 1 accounts are anonymous, may be opened electronically or in retail stores, and require no account opening data. Monthly deposits, however, cannot exceed $291, the balance may not exceed $388, and funds may not be transferred to other accounts. Cash may be deposited only through physical channels.
- Tier 2 accounts require some basic personal information—name, DOB, gender, address, and Mexican state of origin—but also may be opened electronically. Monthly deposits may not exceed $583 and the balance may not exceed $1,165. Electronic banking and mobile transfers may be used.
- Tier 3 accounts require still more personal information—including occupation, phone number, email, and national identity and tax numbers—and may also be opened electronically. The monthly deposits are capped at $3,885, but there is no balance limit.
- Tier 4 accounts are full featured, traditional bank accounts with checking and no deposit or balance limits. Physical presence is required for opening and the financial institution must keep copies of the identification information for a full KYC file.

Though Mexico's financial inclusion numbers have not been buoyed as much as hoped by

[56] A. Newman, *No Address, No ID, and Struggling to Get Their Stimulus Checks*, The New York Times (Apr. 5, 2021).

[57] FATF Guidance at ¶137.

[58] *See* Pew Research Center, *Internet/Broadband Fact Sheet* (Apr. 7 2021); *Mobile Fact Sheet* (Apr. 7, 2021).

[59] *See, e.g.*, USA Today, *Broadband for all: Inside President Biden's $100 billion plan to improve internet access* (Apr. 5, 2021).

III. Clearly define the benefits of digital ID for AML/CFT purposes, including for AML Effectiveness and Financial Inclusion

Though the FATF Guidance has effectively started cataloging many of the benefits of digital ID for AML/CFT,[46] financial institutions and regulators should continue to explore and define them but pay special attention to two key rationales: (1) effectiveness and (2) financial inclusion. These two rationales have now taken on greater significance in the context of recent world events of the COVID-19 pandemic and its economic fallout, as well as AML reform efforts emphasizing the "effectiveness" of AML programs. The FATF Guidance recognizes the importance and interrelatedness of both, suggesting that digital ID systems could not only "generate cost savings" and "help lower onboarding costs" for financial institutions, but also that "[t]hese cost savings could enable regulated entities to allocate compliance resources to other AML/CFT compliance functions, and also facilitate financial inclusion for otherwise excluded or under-served individuals by reducing on-boarding costs."[47]

1. Digital Identity and AML "Effectiveness"

As adopted at the October 2019 BSAAG Plenary and subsequently disseminated by FinCEN's advance notice of proposed rulemaking on AML Program Effectiveness, the BSAAG's AML Effectiveness Working Group identified regulatory initiatives that would allow financial institutions to reallocate resources in order to refocus their AML/CFT programs on more effective and efficient methods of detecting and preventing money laundering.[48] This theme has since been reinforced

---

[46] FATF Guidance at ¶¶104-11 (e.g., minimizing human error, improving customer experience, and enhancing transaction monitoring). Though better defining the risks, their mitigants, and best practices will also of course be critical to the effective use of digital identity in AML/CFT programs, they deserve more extensive consideration and expertise than we can give them here without consultation with broader group of stakeholders, such as cyber and fraud departments from FIs, law enforcement, and digital identity providers. The FATF Guidance effectively catalogs the risks, and their mitigants, of digital identity including the following (many of which may be overlapping): data loss; data corruption; misuse of data due to unauthorized access; cyberattack; impersonation risks; synthetic IDs; authentication and life cycle management risks, including credential stuffing, phishing, man-in-the-middle or credential interception, and PIN code capture and reply; multi-factor authentication vulnerabilities; and bio-metric authenticator spoofing and lower reliability of facial recognition with darker pigmentation or certain types of facial features. Members of this group have reported that their institutions are encountering many variations of these issues already in their fraud prevention efforts, including SIM swapping, IP/geolocation spoofing, cookie copying, browser version and screen resolution emulation. While FATF identifies some mitigants for these risks, technical standard setting bodies like NIST may be best suited to helping FIs control for these risks in the AML context going forward. Of course, many FIs already control for these risks in their fraud and cyber programs and may be well-prepared to understand the risks of incorporating these digital signals in their AML programs. In any event, since risks like these persist both online and in-person and increased digitization of customer relationships is a certainty, the real question for FIs may not be "whether" to consider these digital signals for AML/KYC purposes, but "how".

[47] FATF Guidance at ¶107.

[48] FInCEN, *Advance Notice of Proposed Rulemaking: AML Program Effectiveness*, 85 FR 58023, 58025 (Sept. 2019).

IV. Progressive Identity and the Customer Journey

A. Encourage the use of information associated with digital identification for broader KYC and transaction monitoring purposes

Financial institutions (and their examiners) should take the FATF's cue and expand their view of traditional KYC information to include those "anti-fraud and cyber-security processes to support digital identity proofing and/or authentication for AML/CFT efforts [like] customer identification/verification at onboarding *and ongoing due diligence and transaction monitoring*."[60] Depending on the purpose and stage of the relationship, these "digital signals" may include: geolocation, MAC and IP addresses, biophysical biometric attributes (e.g., fingerprints, iris patterns, voiceprints, facial recognition), biomechanical patterns (e.g., keystroke mechanics, typing cadence, or device angle compared with known patterns), behavioral attributes (e.g., expected log-in channels, email/text message patterns, file access log, time of log-in, etc. compared with historical behavior), email age, patterns of website interaction (e.g., expected progression through product offering and account opening), frequency and type of usage, among others.

Without engaging in the extensive and necessary analyses of the specific use cases and best practices necessary for these digital signals in AML/KYC processes here, the basic use case for digital signals in AML/KYC processes is clear: as customer relationships become increasingly digital, and decreasingly in-person, a customer's behavior online becomes increasingly important to the fundamental CDD undertakings of "understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile [and c]onducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information."[61] The strength of the binding event at onboarding that pairs the registered/identified and verified customer with his/her device(s) can help the financial institution establish the initial level of confidence in the identity and risk of the customer and inform the risk appetite for product and service levels for the customer. Ongoing authentication, "progressive binding" of new devices authenticated by the customer, behavioral trends, and events across the duration of the customer lifecycle may then all contribute to a customer's dynamic KYC profile. By expanding the initial profile of the customer necessary for onboarding, over time the financial institution develops a better understanding of the customer and its risk profile, which in turn allows the financial institution to expand the level or products and services. Merging these digital signals with traditional and evolving transaction monitoring scenarios and techniques will allow

[60] FATF Guidance at ¶26 (emphasis added).

[61] See, e.g., 31 CFR §1020.210(a)(v) (CDD procedures requirement for banks).

financial institutions to better "follow their data" in discerning patterns of suspicious activity, in addition to fraud.

B. Identification and verification are only the beginning—digital identity elements should inform the ongoing CDD obligations to understand the nature and purpose of the customer relationship.

To reap these benefits most effectively, however, financial institutions and regulators should—or at least should have the option to depending on the financial institution's scale and resources—treat digital identification as a dynamic and progressive process of understanding customer identity over time as more data attributes are gathered and/or customer risk changes. Instead of treating identification and verification as a periodic, static, "point in time" check like onboarding followed by KYC refresh intervals, financial institutions, regulators, and examiners should recognize possibility that the continuous process of ongoing and dynamic identity proofing inherent in digital customer relationships may help facilitate different kinds of customer relationships, including more financially inclusive relationships. A dynamic, progressive view of identification would implement trigger-based thresholds in the KYC process that would prompt additional levels of assurance and verification and utilize that data to continuously rescore the overall confidence in the customer identity and, in turn, determine the scope of customer activity. In this KYC paradigm, a customer would progress on their "customer journey" from lower-risk, limited activity, but financially inclusive accounts to increasingly sophisticated products as that confidence increases—a process not dissimilar to today's credit card business models, which raise credit limits as the financial institution's confidence in their customer increases.

But this new paradigm will require reimagination of the customer lifecycle for AML/KYC purposes. Today, traditional customer risk assessment methodologies identify four general categories of "risk factors" that inform the overall profile: (1) intrinsic customer-related factors like professional activity; (2) geographical factors; (3) product, service and transactional behavior like inherent product risk or associated source/destination of funds; and (4) delivery channel such as in person or digital. In a progressive digital identity environment, however, "delivery channel" becomes its own distinct taxonomic rank. Instead of a "factor among many" at onboarding, it becomes the ordering principle for how financial institutions manage the customer across their lifecycle and puts a premium on the financial institution's own technical capabilities and digital transparency between the financial institution and customer, which will likely be determined in some measure by the customer. Thus, if a customer uses a VPN or blocks location permissions—both legitimate privacy-based decisions—the progressive identity of the customer will be hampered (as will the frictionless service) as the financial institution may likely have to resort to more traditional KYC techniques or limit the customer's access to its services.

For progressive identity concepts to be most effective, however, financial institutions should increasingly be able to treat significant deviations in risk factors as triggers for increased levels of assurance. To begin operationalizing those triggers, financial institutions should consider de-constructing each broad risk factor into a series of variables, or data elements, and mapping

those elements to the internal or external digital signals capable of indicating a deviation from the existing value (e.g., as collected at onboarding). Established thresholds against the variable's behavior would then determine whether or not the deviation reflects a material change in the overall risk factor and/or if a specific action is necessary to gain further confidence that the risk profile has actually changed (i.e., the trigger). Initially these thresholds may be theoretical (or vendor-driven based on industry experience), but over time, insights into the digital customer lifecycle management program would facilitate the financial institution's ability to "follow their data" and decrease or increase the need to trigger a specific action. For example, if the IP address login activity for the main account contact changes to be outside of the country(ies) stated at onboarding, the risk profile should be reassessed and updated to reflect this new country of operation.

In this vision of progressive identity, financial institutions should be better equipped to fulfill their fundamental obligation to understand the nature and purpose of their customer relationships on an ongoing basis. Combined with traditional transaction monitoring, financial institutions should be able to identify a more holistic picture of customer risk by focusing less on cruder proxies of customer risk assessed at arbitrary intervals and more on customer behaviors and intent.

C. An explicit provision for simplified due diligence would increase adoption of progressive identity and encourage financial inclusion.

In order to enhance the potential of progressive identity and take full advantage of its potential for financial inclusion, however, U.S. regulators should consider adopting regulations that would encourage a true simplified due diligence (SDD)—a concept that has long been part of the FATF's Recommendations,[62] but currently does not exist in the BSA/AML regime. Though a part of its initial 2012 Recommendations, the FATF more explicitly highlighted the importance of SDD to financial inclusion in its 2017 *Financial Inclusion Guidance*, which encouraged the reliance on a broader range of identification criteria as a part of SDD measures.[63] While the CIP Rules do, as discussed, provide some flexibility in the information collected from customers, they do not clearly tie the possibility of a simplified due diligence in connection with lower risk customers or relationships, products, or services. Regulatory sanction of this concept in the U.S., would encourage financial institutions to take the regulatory risk of "doing less," even if it is proportionate to the lower risks of the customer, for the laudable policy goal of financial inclusion.

V. Next Steps

Without a national government-issued form of digital ID in the U.S., financial institutions and their regulators will need time and flexibility to test new methods to fully realize the potential

[62] FATF, *The FATF Recommendations* ¶21, Interp. Note. to Rec. 10 (2012).

[63] FATF, *FATF Financial Inclusion Guidance* at 20 (2017).

of our digital ID mosaic for AML/CFT purposes. However, this Group believes there are a few key next steps that would accelerate these efforts.

A multi-stakeholder approach. To fully understand and leverage digital ID for AML/CFT, financial institutions, regulators, and law enforcement should include technology and digital identity firms that are actively working on digital identity solutions—either for governments or financial institutions—in the conversation about how to develop and operationalize ideas like progressive identity. Since most digital identification software and systems for financial institutions are currently developed by specialized vendors, financial institutions, regulators, and law enforcement would benefit from greater understanding of the increasingly specialized techniques used by digital identity firms and their application to KYC. Similarly, different government agencies at both the federal and state level that deal with identifying information should be a part of the conversation to identify synergies and areas of collaboration between the public and private stakeholders that share the same goals for digital identification. To fully capture the range of views from these stakeholders, FinCEN should consider issuing a Request for Information (RFI) or an advanced notice of proposed rulemaking (ANPRM) on potential amendments to the CIP Rules, including those discussed above. To facilitate an effective and probing RFI or ANPRM, FinCEN could consider commissioning additional inquiry under the AML Act-mandated BSAAG Subcommittee on Innovation & Technology, possibly in tandem with the Subcommittee on Information Security & Confidentiality, to better define the scope of issues under digital identity and reform of the CIP Rules and better inform an effective RFI or ANPRM on CIP in the future. In addition, FinCEN could consider devoting some portion of the AML Act-mandated Financial Crimes Tech Symposium to the topics of Digital ID and financial inclusion, especially since the AML Act specifically requires the inclusion of international participants, many of whom have addressed these issues more squarely in recent enhancements to their AML/CFT regimes.

Legal entities. While this paper has focused primarily on digital ID in the context of natural persons, digital ID should also be leveraged for legal entities. Certainly, the identification of beneficial owners, control persons, and representatives of legal entities will benefit from advances in the digital identification of natural persons. However, digital identity solutions for entities themselves could also benefit from digital identification. Indeed, the forthcoming beneficial ownership registry required by the CTA could be seen as the foundational data point in the digital identification of legal entities.

Portability. As noted by the FATF, the portability of digital identification—the ability for a customer to utilize their proofed digital identity between different financial institutions—would make it far more valuable.[64] Where a digital identity can travel with a customer between financial institutions, it can allow the customer to continue that "customer journey" of progressive identity uninterrupted through their relationships with different financial institutions without having to

[64] *See* FATF Guidance at ¶168.

start from the beginning, building digital trust with each successive financial institution. Financial institutions would benefit not only from not having to redo a customer's KYC profile at each financial institution of their choice, but also from the accumulated risk information that comes with portability. Portability could also help reduce the constant re-exposure of a customer's personal identifying information (PII) in their onboarding at every financial institution. Again, without a national digital identity platform, the U.S. may be at a structural disadvantage on issues like portability. However, this Group strongly believes in pursuing portable digital identity solutions, and how financial institutions, digital identity providers, and government may be best be incentivized in that pursuit.

Government's Role and Partnership. Composed primarily of industry participants, this Group focused more on what financial institutions themselves can do or how AML/CFT regulations may be changed to enhance and promote the use of digital ID. However, even if a national identification system will always remain the "third rail" of the identification problem, there is unquestionably a greater role for governments to play in an effective digital identification system. While this paper explored the potential for mDLs and the use of their identification numbers above, the possibilities for federal government's role in digital identification should also be more deeply explored. Perhaps because of the national identity debate, the federal government has been viewed more as a technical standard setter—as with NIST's global leadership on the issue—or as a regulator—as with the CIP Rules. However, the federal government has recently taken an important step towards utilizing its powerful imprimatur as an authoritative "source of truth" in the digital ID ecosystem with the introduction and scaling of the Social Security Administration's (SSA) electronic Consent Based Social Security Number Verification (eCBSV) Service.[65] Required by 2018's Economic Growth, Regulatory Relief, and Consumer Protection Act, the eCBSV allows authorized entities, including financial institutions with customer consent, to query the SSA's database and verify if an individual's SSN, name, and date of birth combination matches the SSA's records. While there is of course room for improvement, the rollout of eCBSV is a welcome addition to the suite of digital identity tools for financial institutions and others. We should, however, continue to explore further roles for the unique authority of federal (and state) government in validating identity attributes while ensuring the privacy and control of consumer data.

[65] Social Security Administration, electronic Consent Based Social Security Number Verification (eCBSV) Service.