Center on
Regulation and Markets
at BROOKINGS

Financial Crimes Enforcement Network (FinCEN)
U.S. Department of the Treasury
Policy Division
P.O. Box 39
Vienna, VA 22183
Docket Number FINCEN-2024-0009

To the Policy Division:

In response to FinCEN's request for information (RFI) of March 29, 2024, I offer the following comments. While the RFI is narrowly focused on the methodology banks and third parties use to identify customers through Social Security or Taxpayer Identification numbers (SSNs or TINs), this comment letter suggests core questions that FinCEN should be asking in furtherance of the goals of improving anti-money-laundering (AML) and countering the financing of terrorism (CFT) efforts, while enhancing financial inclusion and the overall health of the financial system. FinCEN and other U.S. financial regulators have too often prioritized questions of *how* to collect more AML/CFT information but lost sight of *why* to do it. FinCEN would be better served by fundamentally rethinking what types of data are needed and how they are collected.

Information on customer identity is collected for both business and regulatory purposes. Financial institutions need to verify the identities of their customers as a prerequisite to providing services, to guard against fraud, and to otherwise understand and manage their firms' own risks. These requirements create substantial but incomplete incentives for firms to verify customer identity. Financial regulators and FinCEN require identity information to carry out various legal and regulatory requirements, including monitoring, detecting, and prosecuting AML/CFT violations. The goal of the regime is to prevent and identify illegal activities and help bring criminals to justice. This is an important addition to private market incentives. FinCEN will be most effective if it considers the combination of these factors and resists being overly proscriptive in its efforts to guard against gaps in identity verification.

Two examples highlight these problems. The first is the recent claim that baseball star Shohei Ohtani was the victim of identity and bank account theft of more than $15 million by his interpreter Ippei Mizuhara. According to an affidavit filed in that case[1], Mr. Mizuhara was able to fake the identity of Mr. Ohtani—one of the most famous athletes in the world—to gain control of his bank account, changing phone numbers and e-mails associated with the account, and subsequently send at least $15,000,000 in wire transfers to account(s) associated with an illegal bookmaker over the course of 18 months. How was it possible for these activities to occur without triggering massive AML concerns regarding customer identity and account activity?

A recent letter led by Senator Jack Reed (D – RI) and joined by six other senators highlighted a second example of regulatory gaps in identity verification. They note the danger posed by regulatory gaps in the coverage of AML/CFT enforcement that exist with investment advisors and private funds. All of these objectives involve inherent risks, such as that customers may provide inaccurate information or try to game identity systems. They also involve substantial costs to improve the accuracy of identification systems targeted primarily to high-net-worth individuals and large dollar volume transactions.

[1] United States of America v. Ippei Mizuhara, United States District Court for the Central District of California Case No. 2:24-mj-02125-DUTY, accessed: https://www.espn.com/prod/styles/pagetype/otl/2024/240411_ent_mlb/2-24MJ2125-complaint-mizuhara.pdf?consent_mode=ccpa

Standard economics assumes that the cost of enhancing accuracy rises as baseline accuracy increases, probably on a non-linear basis. For example, it is more expensive and difficult to raise accuracy from 98% to 99% than from 67% to 68%. Economic logic also suggests there is a point at which the marginal costs of enhanced accuracy exceed the marginal benefits. These costs may or may not be completely borne by the financial institutions charged with identity verification. Consumers bear costs both from the process of proving their identities and from the consequences of being unable to provide required documentation. For some, those costs mean being ineligible for the services they seek, thus being financially excluded.

Financial regulatory agencies are appropriately concerned with consequences of customer identification. A broad set of consumer protection laws, including the Electronic Funds Transfer Act, allocate liability to financial institutions in instances of fraud. This appropriate allocation of property rights (liability of fraud in this case) has resulted in a system in which financial institutions spend billions of dollars a year to counter potential fraud and to correctly identify customers.[2] Congress may do well to revisit some of these laws in light of new methods of payment and new types of fraud, particularly in the case of wire transactions from funds in broker dealers and insured depository institutions.

The important goals of financial stability, consumer protection, combating financial crimes, and building an inclusive financial system require thorough and proactive measures to ensure that innovation is properly understood and that financial institutions and regulators take appropriate safeguards. If policymakers do not consider these goals together, moving forward on one goal risks losing ground on others. For example, increasing barriers to accessing the financial system may reduce money laundering but can unnecessarily decrease financial inclusion if not thoughtfully implemented and properly targeted.

However, technology can also help regulators achieve their goals. It is incumbent upon regulators to embrace new regulatory technology (reg-tech) for good purposes. Unfortunately, much less attention has been paid to the benefits side of the coin. Financial regulators and FinCEN should broaden their focus from not just how financial institutions use technology on issues of identity verification but on how regulators can use technology to enhance their ability to verify that appropriate AML/CFT actions are taking place. Regulators need to guard against relying on outdated technology while allowing financial institutions to use new technology to more efficiently and effectively meet regulatory requirements and business goals.

Failing to adopt new technology leaves old and increasingly outdated systems in place. The correspondent banking system was the backbone of international bank funds transmission for the 20th century. Correspondent banking has faced rising compliance requirements for customer identity verification over the past several decades as AML/CFT laws have continuously added requirements to meet new challenges.[3] Banks heavily rely on the risk management capabilities of correspondents, and banks' uncertainty as to the ability of correspondents to mitigate some risks

---

[2] Aaron Klein, "Adapting regulation for the fintech world" (working paper, Brookings Institution, 2016), brookings.edu/articles/adapting-regulation-for-the-fintech-world/

[3] Kathryn Judge and Anil K. Kashyap, *Anti-Money Laundering: Opportunities for Improvement*. (Philadelphia, Pa: Wharton Initiative on Financial Policy and Regulation, April 2024). 3-10, https://wifpr.wharton.upenn.edu/wp-content/uploads/2024/03/WIFPR-Anti-Money-Laundering-Judge-and-Kashyap.pdf

has led to a trend of de-risking, or terminating relationships with classes of customers, countries, and the like. This is a key mechanism through which AML/CFT regime can limit access to financial services.

According to the latest FDIC statistics, about 4.5% of U.S. households are unbanked. The unbanked rate for Black households with annual incomes between $30,000 and $50,000 is 8.0%, versus 8.4% among Hispanic households and just 1.7% for white households.[4] Notably, lack of identity documentation is more frequently cited among people who are unbanked and employed (15%) than among those who are unemployed (12%) or not in the labor force (9%). This suggests that many who have identity documentation sufficient for employment lack the documentation needed to open a bank account.

The costs of complying with Know Your Customer (KYC) rules as part of AML/CFT efforts drive up the cost for banks to offer basic bank accounts as business try to pass along costs to customers. Customers may see higher minimum balance requirements to qualify for "free checking" and/or higher monthly account fees for accounts that do not meet the minimum average daily balance. The cost of basic banking is the number one reason cited by the unbanked in the FDIC's survey for why they do not have a bank account, and we should understand that AML/KYC compliance costs play a role in increasing the cost of providing basic banking services to lower-income households.

Customers in these groups—often those with lower incomes or in vulnerable groups such as immigrants and migrants—are among the hardest-hit by de-risking. The Global Center on Cooperative Security noted that "[r]ather than reducing risk in the global financial sector, de-risking actually contributes to increased vulnerability by pushing high-risk clients to smaller financial institutions that may lack adequate AML/CFT capacity, or even out of the formal financial sector altogether."[5]

This is not necessarily because these customers are high-risk but often because they provide lower margins and are considered worth less risk to keep as customers. As Judge and Kashyap (2024) conclude: "Given that the private sector will bear some of the reporting and enforcement burden, one (rational) response of the private sector is to exclude potential clients/customers for whom the compliance costs exceed the perceived benefits of serving them."[6] Further, the payment technology underlying the correspondence system has not kept pace with added regulatory burdens. The result is higher costs for users of the system and less-than-ideal performance in AML/CFT efforts that rely on outdated technologies.

It is important to note that financial inclusion improves AML/CFT efforts. Individuals outside the financial system are more difficult to track, and, by definition, they conduct business outside of the well-regulated space. In 2013, the Financial Action Task Force (FATF) released guidance

---

[4] FDIC, "2021 FDIC National Survey of Unbanked and Underbanked Households," July 24, 2023, https://www.fdic.gov/analysis/household-survey/index.html

[5] Michael Barr, Karen Gifford, and Aaron Klein, "Enhancing anti-money laundering and financial access: Can new technology achieve both?" (working paper, Brookings Institution, 2018), 5, https://www.brookings.edu/wp-content/uploads/2018/04/es_20180413_fintech_access.pdf

[6] Kathryn Judge and Anil K. Kashyap, *Anti-Money Laundering: Opportunities for Improvement*. (Philadelphia, Pa: Wharton Initiative on Financial Policy and Regulation, April 2024). 29, https://wifpr.wharton.upenn.edu/wp-content/uploads/2024/03/WIFPR-Anti-Money-Laundering-Judge-and-Kashyap.pdf

(revised in 2017) on how to successfully marry AML/CFT and financial inclusion efforts, warning that an "overly cautious approach to AML/CFT safeguards can have the unintended consequences of excluding legitimate businesses and consumers from the financial system."[7]

FATF promotes a risk-based approach to AML/CFT that directs resources where they can do the most good and contemplates simplified customer due diligence (CDD) requirements for lower-risk individuals. The guidance notes that "newly banked and vulnerable groups often conduct a limited number of basic, low value transactions" and therefore may present a lower risk of money laundering or terrorism financing.

Digital identities involve collecting customer data once and then giving control of how the data collected is used to the customer.[8] This contrasts with the current system, where each service provider must separately collect identity details. The current system is repetitive, expensive, and increases opportunities for fraud. Reducing the number of digits of SSN collection is a small step in the right direction, incorporating digital identity creates opportunities for improvement on which FinCEN should capitalize.

The use of digital IDs can reduce fraud and the incidence of human error in the verification process, increase the security of private customer information, and decrease the potential for discrimination. And by reducing the cost of the verification using a risk-based process, digital IDs can promote financial inclusion and thereby further promote AML/CFT efforts. Indeed, in its 2020 "Guidance on Digital Identity," FATF noted that "digital ID systems that mitigate these risks in accordance with digital ID assurance frameworks and standards hold great promise for strengthening CDD and AML/CFT controls, increasing financial inclusion, improving customer experience, and reducing costs for regulated entities."[9]

Digital identity is a current reality and is growing as a better, faster, cheaper, and more secure system of proving identity. Six states, including Maryland, have already created digital driver's licenses that TSA uses in the critical process of securing air travel.[10] Driver's licenses are the most common form of photo identification in the U.S. It is ironic that FinCEN's RFI focuses on SSN—a nearly 100-year-old form of paper card-based numeric identification—and the question of how to move from using all nine to just four of those digits for verification just when digital identity technology is making rapid advances in both the private and public sectors.

FinCEN and U.S. financial regulators should start embracing digital identity for AML/CFT purposes now. It should be acceptable for banks to embed digital driver's licenses and potentially other widely-used identity sources in their APIs and other security processes to verify ID. If TSA

---

[7] FATF, "FATF Guidance: Anti-money laundering and terrorist financing measures and financial inclusion," (FATF, 2017), 5, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf.coredownload.pdf

[8] Sachin Parate, Hari Prasad Josyula, and Latha Thamma Reddi, "Digital Identity Verification: Transforming KYC Processes in Banking Through Advanced Technology and Enhanced Security Measures." *International Research Journal of Modernization in Engineering Technology and Science* 5, no. 9 (September 2023). https://www.doi.org/10.56726/IRJMETS44476

[9] FATF. "Guidance on digital identity," (FATF, 2020), 9 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf

[10] Secure Technology Alliance, "Implementation Tracker Map," MDL Connection, 2024, https://www.mdlconnection.com/implementation-tracker-map/.

is comfortable enough to use digital licenses for air travel, shouldn't bank regulators be for basic banking?

In addition, fintech can improve collaboration between financial firms and law enforcement agencies by improving the reliability of information and for transmitting it securely while preserving customer privacy.

In a 2018 paper I wrote with Michael Barr and Karen Gifford, we suggested several responsible reforms to the cross-border payments system that would further financial inclusion while also improving AML/CFT efforts.[11] Specifically, we recommended requiring:

1. Settlement for cross-border payments to be completed either the same day or faster, which would reduce opportunities for bad actors to interfere with legitimate transactions and help the most vulnerable potential customers who live paycheck-to-paycheck and would be helped by shorter settlement times.

2. Pre-confirmation of recipient accounts to reduce opportunities for operational failures and fraud and also support other compliance measures.

3. Interoperability of payment systems to lower costs and improve the speed of processing payments.

4. Identity portability to reduce barriers to entry for new service providers, provide greater transparency, and enable individuals to own and control the use of their identity.[12]

While these reforms are not up to FinCEN on its own to propose or implement, FinCEN should be working with other U.S. financial regulatory agencies to advance such reforms that would help it to better do its job.

A good example of a relevant and contemporary rule-making process is the Consumer Financial Protection Bureau's (CFPB's) work to implement Section 1033 of the Dodd-Frank Act. Section 1033 provides that banks and other covered financial institutions must make available to consumers, upon request, transaction data and other information concerning consumer financial products and services provided by those entities. The CFPB is concerned with the privacy and security of consumer data affected by this rule. FinCEN and other regulators with similar goals should work together to become aware of each other's potential concerns and considerations, as well as solutions that can be applied across issues.

New technology involves implementation risks. Yet, failing to innovate results in perpetuating the flaws of the current system. As criminals use new technologies to find ways to circumvent the AML/CFT system, failing to innovate weakens the system, making it more porous and flawed over time. The question should not be whether to allow and expand the use of digital IDs and similar technologies but rather how the U.S. government should go about safely and

---

[11] Michael Barr, Karen Gifford, and Aaron Klein, "Enhancing anti-money laundering and financial access: Can new technology achieve both?" (working paper, Brookings Institution, 2018), 5, https://www.brookings.edu/wp-content/uploads/2018/04/es_20180413_fintech_access.pdf

[12] Ibid, 9-10.

effectively implementing a system that will take advantage of the benefits—including financial inclusion and AML/CFT efforts—that digital ID verification offers. Rather than debating how many digits of a physical card should be used in an identification system created before the transistor, instead focus on incorporating new technology already in use and what is likely to become widely available in the near future. I encourage FinCEN to work with other financial regulators to develop a plan to do so and follow up with additional requests for information related to this work.

Sincerely,

Aaron Klein
Miriam K. Carliner Chair and
Senior Fellow in Economic Studies
The Brookings Institution