FiveBy

ADVISORY

Central Bank Digital Currencies: High Risk? Low Risk? Some Risk? No Risk?

Background

A recent report from the Bank for International Settlements indicates that 86 percent of the world's central banks are considering launching central bank digital currencies (CBDCs)—electronic versions of fiat currencies issued by national governments and backed by central banks that can be stored, transferred, and transmitted by digital payment systems and services. CBDCs can present specific cybersecurity risks, that could endanger consumer privacy and security and become a convenient vehicle to help malign actors evade sanctions, launder the proceeds of crime, or finance terrorist operations. In addition, the advent of CBDCs could degrade the US dollar's standing as the world's reserve currency and facilitate sanctions evasion by malign state actors. However, depending on their design, CBDCs can also lower money laundering and terrorism financing risks, especially if anonymous use of these currencies is limited.

CBDCs Require New Thinking

As more countries test and develop CBDCs, US firms and financial institutions will need to adjust their risk assessments and restructure due diligence and compliance programs to prevent sanctioned parties, fraudsters, and other malign actors from accessing these digital instruments. Compliance teams will need additional, sophisticated, and specialized anti-money laundering/counter-financing of terrorism (AML/CFT), digital currency, and regional expertise to effectively mitigate possible new risks. Money mules, including complicit merchants, could more easily move illicit funds between multiple digital wallets, working to obscure countless small transactions entering the CBDC ecosystem. CBDCs could also make cross-border transactions easier and faster for criminals to move illicit proceeds across multiple jurisdictions.

Fraud and AML/CFT risks—whether higher, lower, or merely different—of CBDCs will depend on each currency's design and administrator, according to the Financial Action Task Force (FATF),which has called for organizations to address the risk associated with money laundering and financing of terrorism in a "forward-looking manner" similar to its recommended approach to stablecoins—digital currencies that are pegged to an asset such as the US dollar, whose value remains relatively steady. Unlike stablecoins, however, FATF does not consider CBDCs a virtual asset, but rather a virtual representation of a nation's fiat currency. FATF anticipates that entities dealing in CBDCs will have the "same AML/CFT obligations as they do with fiat currencies or cash" but warns that "CBDCs could present greater AML/CFT risks" because of their increased portability and anonymity.

- FATF judges that a CBDC has the potential to become a high-value bearer instrument that entitles the holder to rights of ownership without record of transfer or any other transactions, making such instruments attractive to criminals and terrorists looking to hide their assets. FATF applies its standards to CBDCs as with any other form of fiat currency issued by a central bank.

- Criminals will likely undertake intricate money laundering schemes to transact in CBDCs, given their distinct technical features, such as wallet programmability, portability, and ability to conduct microtransactions in amounts less than a penny. Terrorists could also use their supporters' wallets and shift between wallets as needed to continue accessing funds. Although criminals will likely still prefer cash because of its anonymity, the

INFO@FIVEBY.COM
206-800-1700
FIVEBY.COM

risk of money laundering schemes could introduce illicit proceeds into the CDBC system by trading cash or anonymous digital tokens through layers of transactions—the second stage of money laundering.

Sanctions Risk

Depending on the issuing jurisdiction, CBDCs could undermine the dominance of the US dollar in the global financial system, causing US sanctions to lose their bite and providing a means for state actors to circumvent the use of the US dollar. Heavily sanctioned countries including China, Iran, Russia, and Venezuela are actively developing CBDCs, which could be used to bypass the Western financial system. In addition, the United States and its allies could also face a new set of security challenges from rogue regimes that decide to develop CBDCs to circumvent international scrutiny, including a heightened risk of nuclear proliferation. The Biden administration is working to understand China's work to establish a CBDC, or digital yuan (e-CNY) and how the new currency could be used to work around US sanctions.

- China aims to launch the e-CNY by the 2022 Beijing Olympics and "expects to challenge the US dollar's hegemony as the international currency," as well as use the e-CNY to "[blunt] the impact of any sanctions or threats of exclusion both at a country and company level."

- In October 2019, Russia's Finance Ministry announced plans to explore the development of a Russian CBDC that could reduce dependence on the US dollar, resulting in an improved ability to circumvent sanctions. Russia's central bank could start pilots and trials of its CBDC in early 2022, according to central bank head Elvira Nabiullina.

- After launching its failed oil-backed Petro cryptocurrency in 2018, Venezuela announced in February that it wants to develop its own CDBC—a digital bolivar. The design of the digital bolivar will likely have lax AML/KYC controls and limited means for identity verification, judging from Venezuela's previous efforts to circumvent US sanctions with the use of digital currencies and lax controls needed to facilitate funds transfers.

When designing a CBDC, governments must walk a fine line between privacy concerns, fraud and money-laundering mitigation, and know-your-customer and due diligence requirements—a balance, that along with the issuing jurisdiction will determine the CBDC's risk profile. Although the idea of a digital dollar has bipartisan support in the House of Representatives, some in Congress insist that a "trusted third party, such as a court, must be able to unmask participants in a transaction when things go wrong." China's e-CNY will be private, but not anonymous, according to the People's Bank of China, which claims the controllable anonymity will prevent criminal use of the digital currency and ensure the bank can track all payments using the e-CNY. The European Central Bank approved a digital euro development project in July. To mitigate fraud risk, the ECB will either limit the number of digital euros individuals can own or penalize amounts over a specified limit during its pilot phase.

Compliance teams will need to adjust to this new payment method by combining their expertise in AML/CFT typologies with current knowledge about digital payments and currencies to uncover new money laundering schemes and methods as criminal behavior evolves to exploit the features of the CBDC. Automated screening tools (ASTs) could help relieve some of the pressure on compliance teams, but these tools would need regular programming from AML/CFT experts catching the evolving methodologies. This expertise will also be vital in analyzing transactions too complex for ASTs to detect. FiveBy recognizes that CBDCs will represent a new digital currency reality and can help US firms anticipate and navigate new AML/CFT and sanctions evasion methodologies that are likely to challenge compliance programs.