

April 28, 2021

VIRTUAL CURRENCY

A Quick Look at New Regulations to Address National Security Threats in Shell Company and Digital Currency Transactions

By [Mario Mancuso](#), [Sanjay Mullick](#) and [Carrie Schroll](#), *Kirkland & Ellis*

Recently, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) has taken steps to implement two new regulatory regimes designed to address national security threats in modern financial transactions.

In late March 2021, FinCEN closed the comment period on its proposed rules to regulate digital currency, an area in which Treasury's Office of Foreign Assets Control (OFAC) has also been active concerning violations of economic sanctions.

On April 1, FinCEN issued an advanced notice of proposed rulemaking (ANPRM) on regulations imposing new beneficial ownership reporting requirements on corporations and other entities, part of its focus on addressing shell companies and suspicious transactions.

Those involved in diligence for transactions and acquisitions would be well-advised to consider how to bolster internal procedures to prepare for this coming regulatory and enforcement landscape. Here we take a quick look at those developments and provide key takeaways.

See "[Cryptocurrency and Corruption: The Future of FCPA Enforcement?](#)" (Mar. 31, 2021).

Tools to Detect and Prevent National Security Threats

These new rules and proposed rulemakings reflect an effort to provide U.S. government agencies with more effective tools to detect and prevent the threat that novel transaction types and complex organizational structures can pose to U.S. national security. These tools appear designed to protect against circumvention of existing safeguards in the U.S. financial system. At her confirmation hearing, Treasury Secretary Janet Yellen expressed concern that digital currency is used for "illicit financing," and stated that financial crime conducted through shell companies is a "very important problem."

The key situations the tools address include:

1. when "bad actors" can remain anonymous by hiding behind alternative currencies and
2. when non-U.S. actors can disguise their identity by hiding behind shell companies.

See "[Making Corporate Transparency a Global Norm](#)" (Sep. 4, 2019).

Digital Currency Concerns and Developments

The U.S. government is taking steps to address the concern that parties using innovative technologies for financial transactions can bypass restrictions in place for traditional currency.

Regulatory Development

On December 23, 2020, FinCEN issued a Notice of Proposed Rulemaking that would revise reporting and recordkeeping requirements for certain transactions involving convertible virtual currency (CVC) or digital assets with legal tender status (LTDA) (collectively, digital currency), when transactions use an unhosted or “covered” wallet. A wallet is “covered” if it is not hosted by a financial institution, or if it is hosted by one that is not subject to the Bank Secrecy Act (BSA) and is located in identified foreign jurisdictions.

1. **Reporting:** FinCEN proposed adding CVC and LTDA to the definition of “monetary instruments” for purposes of Currency Transaction Reports (CTR) requirements, thereby creating a requirement that banks and money services businesses (MSB) report to FinCEN any digital currency transactions over \$10,000 using an unhosted or other “covered” wallet.
2. **Recordkeeping:** FinCEN proposed that banks and MSBs be required to keep records of any digital currency transactions over \$3,000 using an unhosted or “covered” wallet.
3. **Identity Verification:** Banks and MSBs would need to verify each customer’s identity by collecting their name, address

and identification number, and would need to collect the names and addresses of the customer’s counterparties.

FinCEN accepted public comments until March 28, 2021 and will likely take at least a few months to review before issuing a final rule. It is anticipated the final rule will be similar to the proposed rule, though there may be some changes on the margins in response to industry comments and the transition to a new administration.

Enforcement Actions

Digital currency has also been the focus of enforcement actions by both FinCEN and OFAC.

1. **FinCEN:** FinCEN recently [penalized](#) a Bitcoin “mixer” for enabling customers to engage in anonymous transactions through digital currency wallet addresses, without retaining customer information.
2. **OFAC:** OFAC has mirrored this initiative, announcing settlements with two digital currency providers for failure to block transactions when customer Internet Protocol (IP) addresses suggested location in sanctioned jurisdictions and stressed the harm to national security caused by thousands of such digital currency transactions. In the [enforcement release](#) regarding a digital currency payment processor OFAC stated companies “should understand the sanctions risks associated with providing digital currency services and should take steps necessary to mitigate those risks.”

See [“Virtual Currencies: Opening a New Avenue for Financial Crimes”](#) (Mar. 17, 2021).

Transaction Transparency Concerns and Developments

The U.S. government is also taking steps to address the concern that doing business in the name of anonymous entities can hide the individuals that are actually behind those transactions.

Legislative Development

On January 1, 2021, the Anti-Money Laundering Act of 2020's Corporate Transparency Act (CTA) became law, creating new beneficial ownership reporting requirements.

1. **Information Disclosure:** Corporations and limited liability companies must disclose to FinCEN the name, address, date of birth, and identification number of any natural person with a 25 percent or more beneficial ownership interest in or control over the reporting entity. New entities will need to provide such information at the time of formation, while existing entities will have two years to provide such information.
2. **Information Sharing:** FinCEN has the authority to share the information with law enforcement and other regulators. Reporting entities can also request that FinCEN share the information with financial institutions to respond to know-your-customer (KYC) requests. FinCen will develop a database that will serve as a repository of identifying information.
3. **Exemptions:** The CTA excludes many types of entities from the reporting requirements, particularly those subject to similar reporting requirements under other regimes, including certain private

equity investment advisers, including, but not limited to:

- public companies, as well as companies that employ more than 20 people, have filed a tax return reporting gross receipts in excess of \$5 million, and have a U.S. office;
- registered investment companies, investment advisers and certain pooled investment vehicles; and
- entities owned or controlled by exempt entities are themselves also exempt.

A Preview of FinCen's CTA Priorities

The April 1, 2021, ANPRM seeks public input on implementing the CTA. FinCEN has until January 1, 2022, to issue implementing regulations, after which the ANPRM states FinCEN expects to provide additional time for regulated parties to comply. Nevertheless, the [proposed rule](#) demonstrates that FinCEN views implementation of the CTA as a "top priority" and considers the new beneficial ownership database essential to "facilitating important national security, intelligence, and law enforcement activity."

Questions FinCEN raises in the ANPRM preview some of FinCEN's areas of focus, such as:

1. **Affiliated Parties:** FinCEN seeks input on the scope of information that reporting entities must provide with the beneficial ownership information, including whether entities must provide information about affiliates, parents and subsidiaries.
 - FinCEN notes that, given there may be many corporate layers, such

information can be relevant to understanding complex ownership structures.

- FinCEN asks whether such additional information should always be provided or only when it has a bearing on the ultimate beneficial owner, weighing its probative value against the additional administrative burden.

2. **Intelligence Gathering:** FinCEN also expresses interest in how to share information it captures.

- FinCEN raises questions about how to leverage existing technology, including e-filing and online databases, to efficiently disseminate information to other governmental agencies and to financial institutions, to aid their own investigation functions and customer due diligence obligations.
- FinCEN asks whether the BSA's existing provisions are sufficient to safeguard authorized use of the information, reminding that it will be provided to other U.S. government stakeholders involved in national security, intelligence or law enforcement.

non-U.S. persons and start assessing what changes to their internal procedures are needed.

3. It can be expected that regulators like FinCEN and OFAC will play an increasingly active role in addressing national security risks in the U.S. financial system, coordinating to combat corruption, fraud, money laundering and evasion of economic sanctions.
4. A strong compliance infrastructure that includes detailed KYC and recordkeeping procedures will help companies comply not only with these new rules, but also with overlapping requirements imposed by other regulators.

See "[What to Expect From the Biden Administration's New Anti-Corruption Tools](#)" (Mar. 3, 2021).

Key Takeaways

1. The U.S. government is placing greater focus on identifying and controlling non-U.S. actors in the U.S. economy.
2. Companies and financial services providers should examine their ties to

Mario Mancuso is a partner in Kirkland & Ellis' Washington, D.C., office and leads the firm's international trade and national security practice. His practice focuses on guiding private equity sponsors and companies through the CFIUS process and resolving crises involving economic sanctions and export control-related investigations by the U.S. government.

Sanjay Mullick is a partner in Kirkland & Ellis' Washington, D.C., office. His practice focuses on representing clients on investigative, regulatory and transactional matters related to economic sanctions, export and import controls, anti-money laundering and anti-corruption.

Carrie Schroll is an associate in Kirkland & Ellis' Washington, D.C., office. Her practice focuses on export controls, trade and economic sanctions, customs, CFIUS reviews, anti-boycott restrictions, anti-money laundering regulations and FCPA compliance.