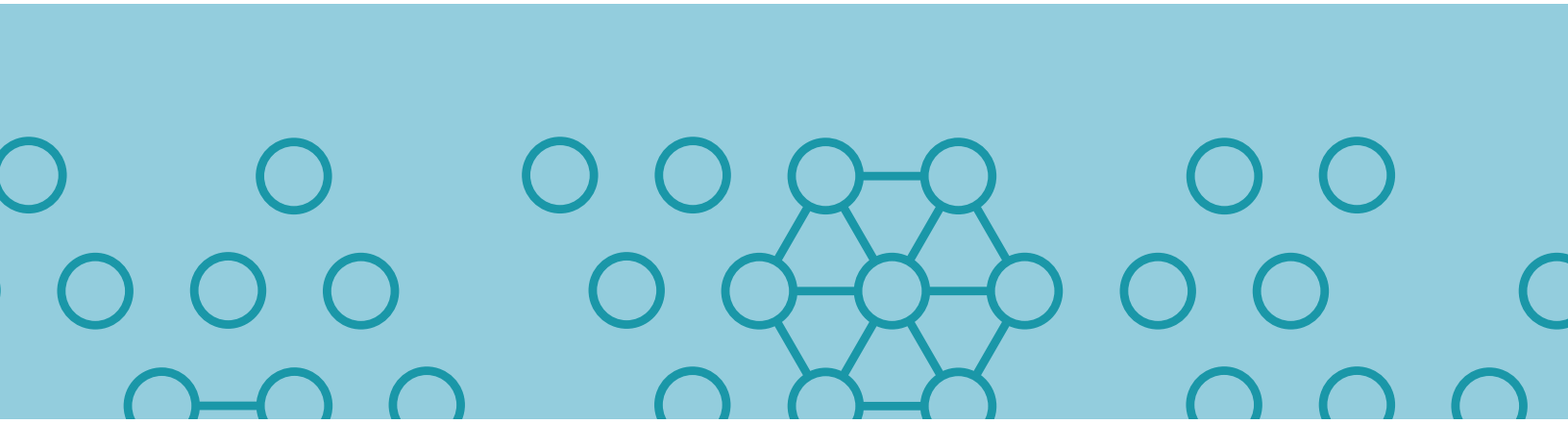
AlixPartners

FINANCIAL SERVICES

MAY 2018

In the 'wild west' of virtual currencies, anti-money laundering and sanctions enforcement is anything but virtual



The numbers of virtual currencies and exchanges have grown explosively in recent years as investors recognize the possibilities in these currencies and the underlying blockchain technology.

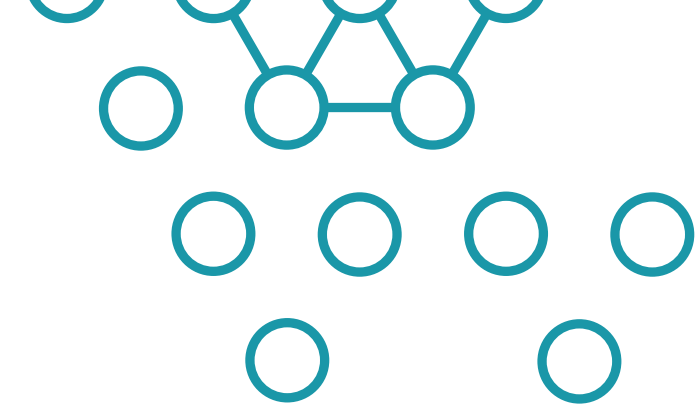
Many banks have begun to explore ways of operating in this space as their clients have tiptoed into cryptocurrencies and blockchain. Doing so, however, brings challenges that are unique to virtual currencies that these institutions must focus on. And the risks for banks should they get this wrong are high.

Regulators have long been concerned about their capacity to be exploited for criminal activity, as made infamously famous by the Silk Road Marketplace[1], and are in the process of developing regimes to monitor and control activity. As virtual currencies, have commanded increasing regulatory and media attention, two popular opinions have emerged:

- They are the wave of the future for payment systems.
- They provide a new innovative tool for criminals, terrorists and sanctions evaders to launder funds.

Europol, Europe's police agency, estimates that 3 to 4% of the continent's annual criminal takings, or $4.2 to $5.6 billion, are crypto-laundered.[2] While mainstream media has only recently begun focusing on money laundering and terrorist financing activities,

[1] https://en.wikipedia.org/wiki/Silk_Road_(marketplace).
[2] Source: *Crypto money-laundering* https://www.economist.com/news/finance-and-economics/21741190-will-crypto-help-money-launderers-future-crypto-money-laundering.



> Because virtual currencies are traded online, there is no face-to-face interaction, and some may permit anonymous and/or strawman funding.

in the recent past there have been some high-profile enforcement actions against virtual currency exchanges, and we expect to see an increasing number of these cases in the coming months and years.

Like other new payment methods, virtual currencies have legitimate uses. They have the potential to improve payment efficiency and reduce per transaction costs for fund transfers. For example, a transaction using Bitcoin can be processed more cheaply than via traditional payment methods or credit card transactions.

However, some of the advantages of virtual currencies also pose the greatest risks that they will be used for money laundering and/or terrorist financing. Virtual currencies can potentially facilitate greater anonymity than traditional payment methods. Because virtual currencies are traded online, there is no face-to-face interaction, and some may permit anonymous[3] and/or strawman funding[4]. Also, obscured transfers are possible if sender and recipient are not adequately identified.

US REGULATORY FRAMEWORK

Virtual currency exchange operators are regulated in the US as Money Services Businesses (MSBs)[5] with the obligation to register with Financial Crimes Enforcement Network (FinCEN) and creating an obligation under the Bank Secrecy Act (BSA) and the USA Patriot Act. Although the individual risk profiles of each virtual currency exchange may vary, often (like other MSBs) they present a generally heightened risk for money laundering, terrorist financing, facilitation of corruption and sanctions evasion.

Every virtual currency exchange must have a risk-based program in place consisting of the following four pillars:

- Development of risk-based internal policies, procedures, and related controls.
- Designation of a responsible compliance officer with sufficient authority.
- Ongoing training.
- Independent testing of the BSA/anti-money laundering (AML) compliance program.

As with most financial institutions, to be compliant with US AML regulations, a virtual exchange should conduct a thorough risk assessment of its products, customers, geographies that considers the risk of money laundering, terrorist financing, sanctions and bribery risks. It should also design a system of internal controls and supporting systems that focus on robust Know Your Customer (KYC) controls. This is especially important at the point when an exchanged from/to virtual currency for fiat currency occurs. The detection and subsequent reporting of suspicious activity can represent significant challenges for virtual currency exchanges and should focus not only on traditional detection patterns but also consider alternative typologies tailored to the virtual currencies, their users and geographies in which they operate.

THE BANKING PERSPECTIVE

Under current US rules and regulations, banks must conduct Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) on virtual currency operators. Due to the heightened risk for AML and sanctions presented by virtual currency

[3] Cash funding.
[4] Third party funding.
[5] Source: https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

exchanges, banks considering taking on these firms as customers must conduct EDD similar to that done with correspondent banking or other intermediary relationships.

Some of the key questions every bank should consider when evaluating a virtual currency exchange include:

- Has the virtual currency exchange established a culture of compliance throughout the organization, or are there organizational silos that inhibit a more integrated compliance approach?
- Has management established appropriate incentives to incorporate AML compliance objectives across the organization?
- Does senior management set the tone through active engagement and involvement in AML risk mitigation?
- Are the exchange's policies and procedures aligned with the business's operating model, and its various lines of business?
- Does management have a holistic view of its customers across geographies?
- Are the various reporting, technological, and other systems integrated geographically?
- Is ongoing compliance monitoring and testing sufficient to identify potential weaknesses?

ANTI-MONEY LAUNDERING ENFORCEMENT IS REAL FOR VIRTUAL CURRENCIES

High-profile enforcement actions in the virtual currency space have drawn significant press attention, and we anticipate seeing more of these in the coming months and years.

Liberty Reserve S.A.

Often cited as the largest online money laundering case in history[6], in 2013, the US charged Liberty Reserve, a Costa Rican based money transmitter, with operating an unregistered money transmitter business and money laundering for facilitating the movement of more than $6 billion in illicit proceeds. Simultaneously, the Department of the Treasury identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act[7], effectively cutting it off from the US and global financial system.

Operating on a large scale, Liberty Reserve had more than a million users globally and handled approximately 55 million transactions. It had its own virtual currency, the Liberty Dollar, but at each end the transactions were denominated in US Dollars.

Users had to open accounts online to conduct transactions through the Liberty Dollar. While Liberty Reserve required basic identifying information, the information provided was not validated by Liberty Reserve, allowing users to establish accounts with fake names ('Russia Hackers,' 'Hacker Account,' 'Joe Bogus') and obviously fake addresses ('123 Fake Main Street, Completely Made Up City, New York').

An additional layer designed to preserve the user's anonymity was the requirement to make deposits and withdrawals through "recommended" third party money transmitters in Russia and several other countries. These companies were often unregistered and operated in countries like Malaysia, Nigeria and Vietnam that had little to no government money laundering oversight at the time.

Once an account was established, a user could conduct transactions with other Liberty Reserve users by transferring Liberty Dollars from his account to other users. For an additional "privacy fee," users could hide their Liberty Reserve account numbers when transferring funds, making the transfers completely untraceable.

Ripple Labs Inc.

In 2015, the FinCEN fined[8] cryptocurrency exchange Ripple Labs, Inc. $700,000 for failing to register with FinCEN as an MSB and for failing to implement and maintain an AML program designed to protect its virtual currency from use by money launderers or terrorist financiers.

[6] Source: https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-liberty-reserve-one-world-s-largest.
[7] Source: https://www.treasury.gov/press-center/press-releases/Pages/jl1956.aspx.
[8] Source: https://www.fincen.gov/sites/default/files/enforcement_action/2016-08-02/20150505.pdf.

BTC-e

In 2017, FinCEN fined BTC-e $110 million[9] for violations of US AML laws. BTC-e was an internet-based, foreign-located money transmitter that exchanged fiat currency as well as the convertible virtual currencies Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum, and Dash. It was one of the largest virtual currency exchanges by volume in the world at the time. BTC-e facilitated transactions involving ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking.

SANCTIONS COMPLIANCE AND ASSOCIATED CHALLENGES

Sanctions risk involving virtual currencies has significantly gone beyond traditional approaches to sanctions compliance with the issuance of a new Executive Order[10] by President Trump on March 19, 2018, expanding the scope of the Venezuela sanctions. The Executive Order prohibits US persons from dealing in any digital currency issued by, for, or on behalf of the Government of Venezuela on or after January 9, 2018, including the 'petro' and 'petrogold.' At the same time and for the first time in history, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) issued FAQs related to the Executive order, as well as new frequently asked questions related to digital currencies[11]. Notably, the FAQs define virtual currencies as follows:

For purposes of OFAC sanctions programs, what do the terms 'virtual currency,' 'digital currency,' 'digital currency wallet,' and 'digital currency address' mean?

- **Virtual currency** is a digital representation of value that functions as (i) a medium of exchange; (ii) a unit of account; and/or (iii) a store of value; is neither issued nor guaranteed by any jurisdiction; and does not have legal tender status in any jurisdiction.
- **Digital currency** includes sovereign cryptocurrency, virtual currency (non-fiat), and a digital representation of fiat currency.
- **A digital currency wallet** is a software application (or other mechanism) that provides a means for holding, storing, and transferring digital currency. A wallet holds the user's digital currency addresses, which allow the user to receive digital currency, and private keys, which allow the user to transfer digital currency. The wallet also maintains the user's digital currency balance. A wallet provider is a person (individual or entity) that provides the software to create and manage wallets, which users can download. A hosted wallet provider is a business that creates and stores a digital currency wallet on behalf of a customer. Most hosted wallets also offer exchange and payments services to facilitate participation in a digital currency system by users.
- **A digital currency address** is an alphanumeric identifier that represents a potential destination for a digital currency transfer. A digital currency address is associated with a digital currency wallet."

OFAC's FAQs further clarifies the obligations relating to virtual currencies as follows that OFAC obligations "are the same. US persons (and persons otherwise subject to OFAC jurisdiction) must ensure that they block the property and interests in property of persons named on OFAC's SDN List[12] or any entity owned in the aggregate, directly or indirectly, 50% or more by one or more blocked persons, and that they do not engage in trade or other transactions with such persons." Adding that OFAC may "include as identifiers on the SDN List specific digital currency addresses associated with blocked persons."

The FAQs seem to expand the virtual currency operators obligations further, stating that "Parties who identify digital currency identifiers or wallets that they believe are owned by, or otherwise associated with, an SDN and hold such property should take the necessary steps to block the relevant digital currency and file a report with OFAC that includes information about the wallet's or address's ownership, and any other relevant details."

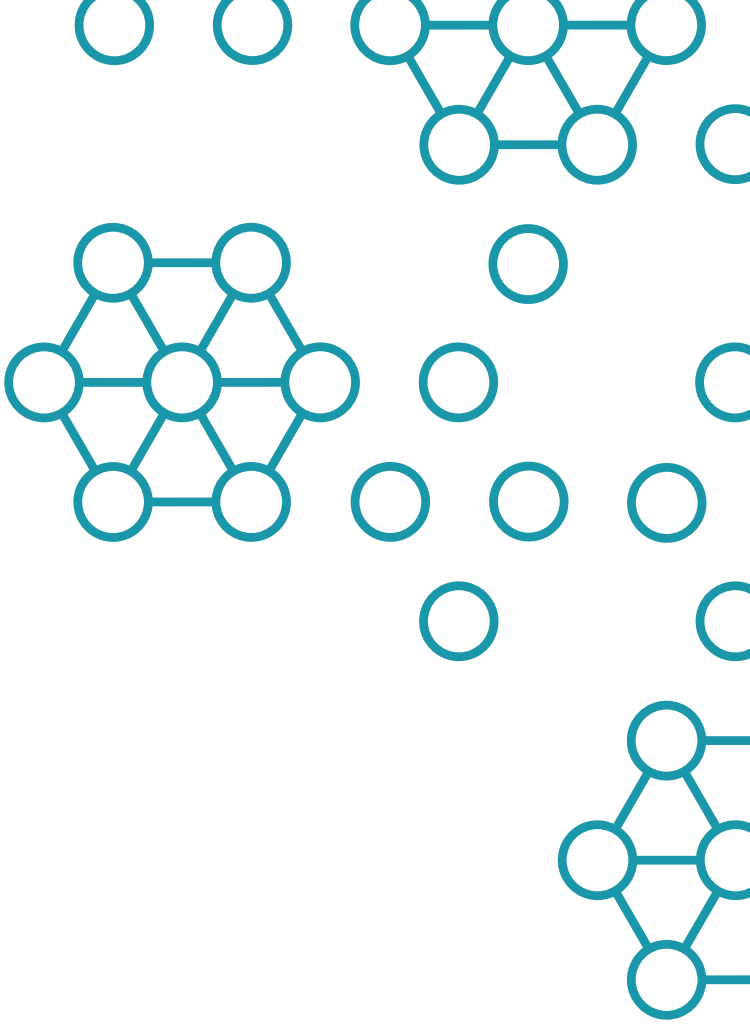
While the Executive Order Seems to be aimed solely against Venezuela, other jurisdictions subject to US sanctions like Russia, could come into the crosshairs as well.

[9] Source: https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware.
[10] Source: https://www.gpo.gov/fdsys/pkg/FR-2018-03-21/pdf/2018-05916.pdf.
[11] https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx.
[12] https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

The related FAQs could have potentially significant implications for virtual currency operators since it signals OFAC's focus on the use of digital currency to circumvent economic sanctions and its active steps to attempt to counter it. This step by OFAC will create new compliance challenges for virtual currency operators, especially considering the implied obligation to link current SDNs to virtual currency identifiers.

LOOKING AHEAD

While virtual currencies offer many opportunities to revolutionize the current financial and commerce system, equally great risks exist relating to money laundering, sanctions compliance, and terrorist financing. Banks and virtual currency operators that can achieve robust levels of AML and sanctions compliance and overcome the various compliance challenges will likely reap the rewards in the future. **A**



CONTACT THE AUTHOR:

Sven Stumbauer

FOR MORE INFORMATION, CONTACT:

Sven Stumbauer
Managing Director
+1 212 845 4044
sstumbauer@alixpartners.com

ABOUT US

In today's fast paced global market timing is everything. You want to protect, grow or transform your business. To meet these challenges we offer clients small teams of highly qualified experts with profound sector and operational insight. Our clients include corporate boards and management, law firms, investment banks, investors and others who appreciate the candor, dedication, and transformative expertise of our teams. We will ensure insight drives action at that exact moment that is critical for success. *When it really matters.*[SM] alixpartners.com