

### Federal Regulatory Regime

- + August 2015 Administrative Ruling on Persons Issuing Physical or Digital Negotiable Certificates of Ownership of Precious Metals;
- + January 2014 Administrative Ruling on the Definition of User in Context of Mining;
- + January 2014 Administrative Ruling on the Definition of User in Context of Software Development and Investing in Virtual Currencies;
- + April 2014 Administrative Ruling on Rental of Computer System for Mining Virtual Currency;
- + October 2014 Administrative Ruling on Virtual Currency Trading Platform;
- + October 2014 Administrative Ruling on Virtual Currency Payment System;
- + March 2013 Guidance (FIN-2013-G001)(“Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,”) In the application of FinCEN’s regulations to transactions in virtual currencies; and In its Guidance, FinCEN refers to the participants in generic virtual currency arrangements, using the terms “exchanger,” “administrator,” and “user.”

■ An “**exchanger**” is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency.

■ An “**administrator**” is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.

■ A “**user**” is a person that obtains virtual currency to purchase goods or services

- + In 2011, Final Rule amending definitions and other regulations relating to money services businesses to provide that money transmission covers the acceptance and transmission of value that substitutes for currency (e.g. virtual currency).

### Texas Regulatory Regime

#### Supervisory Memorandum 1037 (April 3, 2014)

#### **Regulatory Treatment of Virtual Currencies Under the Texas Money Services Act**

Two important findings: (1) Exchanging virtual currency for sovereign currency is not currency exchange under the Texas Finance Code. (Finance Code §151.501(b)(1)); and (2) [M]oney transmission licensing determinations regarding transactions with cryptocurrency turn on the single question of whether cryptocurrencies should be considered “money or monetary value” under the Money Services Act. ... [C]ryptocurrencies, as currently implemented, cannot be considered money or monetary value under the Money Services Act.

### Suggested Approach

#### **1. Identify the customer**

#### **2. Verify Identification**

#### **3. Determine if “bankable”**

#### **4. Evaluate RISK/decide if you want to bank**

- A. Does your customer know who their customers are? Once customer identity is attained, is it verified? How?
- B. Once the customer is identified and the ID is verified, is this a customer you can bank?
- C. Even if you can bank this customer, is it someone you want to bank?

FIs should approach services and customers connected to cryptocurrency with a full understanding of their respective roles with cryptocurrencies and any potential elevated risks. As with any new line of business, the central AML compliance question for FIs should be whether they can reasonably manage their risk. FIs that choose to serve new lines of business or customer types should perform a risk assessment so that they can tailor policies and procedures to ensure that AML obligations can still be fulfilled in the cryptocurrency context.

**From a BSA/AML compliance perspective, an effective crypto-compliance program should include:**

1. The “default” compliance = Following regulatory guidance that applies to MSBs, including the basic elements of KYC, monitoring, prevention, detection, and reporting. This will include:

- Limits or prohibitions on amounts of purchase within a specific time frame (velocity or speed of fund use).
- Controls on the amount of bitcoins purchased by one individual/entity.
- Maximum dollar thresholds on bitcoin ATMs and on the number of transactions within a specific time frame (velocity or speed of fund use).
- Limits or prohibitions on certain usage (e.g., merchant type) and on geographic usage, such as outside the United States.
- Know the identity & location of all third parties involved in the cryptocurrency program, including all agents and any subagents.
- Obtain corporate documentation, licenses, references (including independent reporting services), and, as appropriate, documentation on principal owners.
- Understand the nature of the third-parties’ businesses and the markets and customer bases served.
- Collect information to identify and verify customer identity (KYC)
- Understand the type, purpose, and anticipated use of cryptocurrencies
- Obtain information to fully understand the nature & duration of the relationship with any third parties

2. A system of review that validates customer behavior in conjunction with information gained through a robust customer due diligence process.

3. Consistent blockchain monitoring (i.e. blockchain analysis) to detect potentially illicit transactions through connector tracking and plain text (keyword) analysis, as well as digital wallet connection.

4. Setting practical thresholds and calibrating transaction alert thresholds to account for the current volatility of cryptocurrency values.

5. In addition, onboarding and risk assessment for a cryptocurrency business should include the following questions related to the business’s compliance with applicable regulatory requirements:

– **Information gathering:** Does the customer’s business and compliance model permit it to collect information sufficient to perform CIP and to risk rate its own customers? Does it permit it to obtain information as to counterparties and the locations of transactions?

– **Monitoring and reporting:** Does the customer have mechanisms in place for account monitoring and procedures in place for required reporting?

– **Geographic controls:** Is the service able to control the jurisdictions in which its services are accessed?

– **Legal status and licensing and registration compliance:** Has the service assessed the legality of its services in all the jurisdictions in which it operates?