BANKS' CUSTOMER DUE DILIGENCE OBLIGATIONS AND EXPECTATIONS FOR VIRTUAL CURRENCY RELATIONSHIPS

Mariel Diaz

TABLE OF CONTENTS

EXECUTIVE SUMMARY

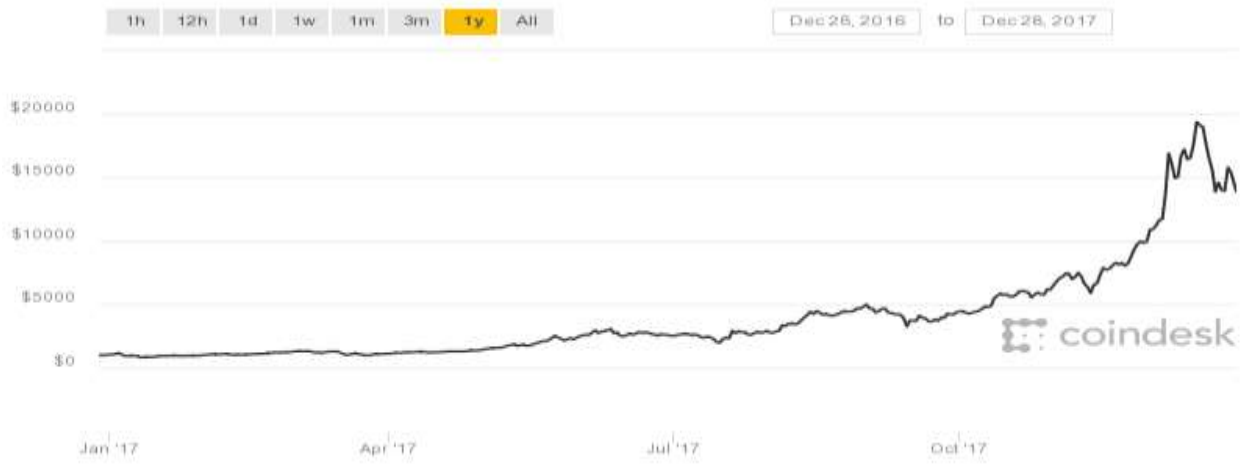
Money transmitters are classified as money service businesses (MSBs) and have been around for many years. Due to several factors, such as being cash-intensive businesses and having a large itinerant walk-in customer base, they are considered high-risk customers by financial institutions where they maintain banking relationships. Even though banks know and understand how the business operates, they have been taking the approach of de-risking money transmitters mostly due to the high level of due diligence required, the resources needed to perform such due diligence, and the costs associated with them. Now per the Financial Crimes Enforcement Network (FinCEN) guidance on virtual currency exchangers (VCEs), VCEs are also considered money transmitters, but a type of money transmitter that transmits a different kind of currency and provides services for totally different reasons and by completely different means. For example, traditional money transmitters' customers are mostly known to use the services to send money abroad to provide financial support to their families. Meanwhile, VCEs' customers are mostly known to use the exchangers to buy virtual currency as investments or speculation.

VCEs already pose money-laundering and/or terrorist-financing risks to banks merely for being a relatively new business type within the industry. While banks are working on understanding VCEs' complex business structure, and regulators are working on implementing and/or adapting current regulations to VCEs and providing guidance to banks on how to monitor VCEs to mitigate such risks, criminals are taking advantage of the lack of understanding, controls, and guidance to use virtual currency for funding their criminal activity and launder their proceeds. Now many questions arise as to how this FinCEN classification of VCEs as money transmitters will impact a bank's decision of whether or not to provide services to VCEs and, if so, what kind of due diligence should be conducted on this type of MSB.

This white paper will provide an overview of virtual currency in general, how this new currency interrelates with the banking system, how VCEs are regulated, whether VCEs are higher or lower risk than traditional MSBs, and what level of due diligence is expected from banks that have VCE customers.

INTRODUCTION

Almost a decade ago, we started to hear about a new form of currency that was going to revolutionize the economy as we know it. At first, banks reacted cautiously. From the launch of Bitcoin in 2009, the first cryptocurrency, virtual currencies were merely the province of a few. That all changed in January 2017 when the price of Bitcoin started to climb and went from below $1,000 to almost $20,000 by the end of the year.



Source: *Coindesk*

Even though there are over 2,000 cryptocurrencies issued as of November 10, 2018, with a total market cap of $213,860,820,192, as reported by Coinmarketcap.com, cryptocurrency is still a relatively new product, and people are still unfamiliar with its use and features. In addition, banks, law enforcement, and regulators are still trying to get their heads around the preventive measures for the money-laundering and terrorist-financing risks associated with it.

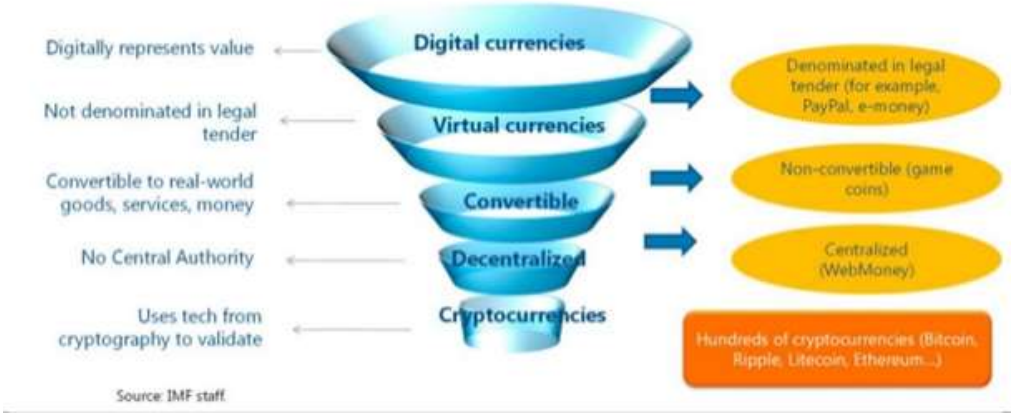
While *cryptocurrency* is a term frequently used by most when referring to digital currency, possibly because the best-known digital currency, Bitcoin, is a cryptocurrency, cryptocurrency is only a subcategory of this new form of money.

Digital-Virtual-Crypto Currency Defined

Digital Currency is a currency available in digital or electronic form, including the representation in electronic format of the fiat currency, which is the currency issued by a government or jurisdiction.

Virtual Currency is the digital currency that is only available in electronic form and does not include fiat currency (i.e., cryptocurrency, coins from virtual games, etc.).

Cryptocurrency is an encrypted virtual currency, hence the name "crypto," that is designed to work as the fiat currency but, unlike fiat currency, is not regulated or backed by any government or jurisdiction (i.e., Bitcoin, Ethereum, Litecoin, Monero, Dash, Zcash, etc.).



Source: *IMF Staff*

Virtual currencies can be convertible or nonconvertible. Convertible Virtual Currency is a virtual currency that either has an equivalent value in real currency or acts as a substitute for real currency. Bitcoin is the best-known convertible virtual currency.

Cryptocurrency Key Features and Characteristics

- ✓ **Digital** – Easily and safely transportable (stored in a digital wallet that can only be accessed by the holder of a private key).
- ✓ **Global** – Allows quicker funds availability with no exchange fees resulting with better payment efficiency and lower transaction costs.
- ✓ **Security** – Encrypted or encoded. Transactions are recorded in the blockchain, which is a digital ledger that records all cryptocurrency transactions. The transactions are stored chronologically and transmitted instantly to networks around the globe. Although transactions on the blockchain are publicly available, they cannot be changed, modified or reversed.
- ✓ **Privacy** – When a cryptocurrency transaction is processed, a pseudonymous identity is created allowing for the real identity of the sender and recipient to remain private.

How Can Virtual Currencies Be Obtained?

One way virtual currencies can be obtained is as a result of mining the digital currency. Mining cryptocurrencies is the process of confirming the validity of a transaction. When a cryptocurrency transaction is sent, the miners receive a very complicated computerized puzzle that needs to be

solved. Whoever solves the puzzle first forwards the solution back to all miners for verification. If all miners obtain the same answer when solving the puzzle, then the transaction is said to be valid and is recorded in the blockchain. The miner who found the solution gets rewarded in the form of cryptocurrency. Other ways to obtain virtual currency are by trading virtual currencies with one another, or by buying the currency with fiat currency via banking transactions, such as wire transfers, ACHs, debit or credit card transactions, etc., or with cash or credit card through Bitcoin ATMs (BTMs).

The most convenient way to initially obtain virtual currency is still by buying the currency with fiat currency. Some virtual currencies can be converted back to fiat currency; therefore, banks can be involved in the process at either the ingress or egress point of the transaction. For this reason, banks should get an understanding of the process in order to implement the necessary controls to prevent their institution from being used to transact illicit money.

WHAT ARE VIRTUAL CURRENCY EXCHANGERS?

Virtual currencies are traded for real currency or other virtual currency through businesses referred to as virtual currency exchangers (VCEs). This is done using an exchanger's online exchange platform or at physical locations through use of a Bitcoin ATM.

Under the Financial Crimes Enforcement Network (FinCEN) guidance issued in March 2013, FinCEN 2013-G001, VCEs are considered money transmitters. The guidance provides a definition for users, administrators, and exchangers of virtual currency, and explains whether or not each classification is subject to regulations. It specifically states that administrators and exchangers are classified as money transmitters and, therefore, are subject to FinCEN and Bank Secrecy Act (BSA) requirements for MSBs.

TRADITIONAL MONEY TRANSMITTERS VS VIRTUAL CURRENCY EXCHANGERS

What Are the Regulatory Requirements for Virtual Currency Exchangers as MSBs?

As per the Bank Secrecy Act regulations, money transmitters are required to:

1. Register with FinCEN and maintain a list of agents (This usually does not apply to VCEs since they typically do not have agents).
2. Obtain a money transmitter license or registration from each state in which they operate (Some states have determined VCEs are not required to be licensed as money transmitters).

3. Establish an anti-money laundering program, inclusive of the original four pillars, but not the fifth pillar, Customer Due Diligence (CDD), since it does not apply to MSBs as explained further in the "Virtual Currency Exchange Relationships" section of this paper.
4. Comply with Subpart F of the regulations on Special Standards of Diligence, Prohibitions, and Special Measures. Money transmitters must implement a due diligence program for agent monitoring[1]. (Since VCEs typically do not have agents, this provision may not apply.)

Who Else Regulates Virtual Currency Exchangers (i.e., states, other countries, etc.)?

The United States is one of the early adopters of this emerging technology and practically marked the beginning of virtual currency regulations. Additionally, the New York State Department of Financial Services (NYSDFS) issued the Final Rule 23 NYCRR Part 200 Virtual Currencies (updated 10/19/2018) requiring a BitLicense[2] for "any Person engaged in any Virtual Currency Business Activity" within 45 days of the effective date of the regulation of June 24, 2015.

In addition to complying with the BSA and state license requirements as money transmitters, where applicable, depending on the type and use of the currency offered by the VCE, VCEs may also be required to register with the Commodities Futures Trading Commission (CFTC)[3] [4] and the U.S. Securities and Exchange Commissions[5] [6] (SEC) as a National Securities Exchange, or be exempt from registration through alternative trading system (ATS).[7] If so, VCEs would also have to comply with securities regulations[8] for each state in which they operate.

As is true of all MSBs, the Internal Revenue Service (IRS) is the delegated BSA examiner of VCEs.

The article written by Matthew Kohen and Justin Wales, co-chairs of Carlton Fields' Blockchain and Digital Currency practice, outlines the regulatory measures taken by each state of the United

---

[1] "Guidance on Existing AML Program Rule Compliance ..." FinCEN. https://www.fincen.gov/resources/statutes-regulations/guidance/guidance-existing-aml-program-rule-compliance-obligations. Accessed December 1, 2018.

[2] "Virtual Currency Business Activity (BitLicense)," NYSDFS. https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses

[3] "An Introduction to Virtual Currency," U.S. Commodity Futures Trading Commission, March 17, 2018. https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/oceo_aivc0218.pdf. Accessed December 1, 2018.

[4] "CFTC Staff Issues Advisory for Virtual Currency Products," U.S. Commodity Futures Trading Commission, May 21, 2018. https://www.cftc.gov/PressRoom/PressReleases/7731-18. Accessed December 1, 2018.

[5] "If a platform offers trading of digital assets that are securities and operates as an 'exchange,' as defined by the federal securities laws, then the platform must register with the SEC as a national securities exchange or be exempt from registration," SEC, March 7, 2018. https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading. Accessed December 1, 2018.

[6] "Statement on Digital Asset Securities Issuance and Trading," SEC, November 16, 2018. https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading. Accessed December 1, 2018.

[7] "Alternative Trading System ("ATS") List," SEC, January 30, 2009. https://www.sec.gov/foia/docs/atslist.htm. Accessed December 1, 2018.

[8] "State Securities Regulators," FINRA. http://www.finra.org/investors/state-securities-regulators. Accessed December 1, 2018.

States as of its publication date of January 9, 2019. Alabama, Connecticut, Hawaii, Idaho, Louisiana, New York, North Carolina, Vermont, Virginia, and Washington have all determined that a money transmitter license is required for VCEs. Alaska, Tennessee, Texas, and Wyoming have decided that a money transmitter license is not required. As for the rest of the states, there is no specific guidance, regulation, or statute addressing licensing requirements for VCEs, and some are working on either modifying or implementing new regulations.

The chart below summarizes the comparison made between traditional money transmitters and virtual currency exchangers:

Traditional Money Transmitters (TMTs) vs. Virtual Currency Exchangers (VCEs)		
Requirement	**TMTs**	**VCEs**
Register with FinCEN	Yes	Yes
Maintain a list of agents	Yes	Typically no
Money transmitter state license or registration required	Yes	Not required for some states TMTs required to be licensed
Establish AML program	Yes	Yes
Due diligence program for agent monitoring	Yes	Usually no
Comply with the new CDD rule	No	No
BSA examiner	IRS	IRS
Other regulators	N/A	CFTC & SEC, when applicable

A QUICK VIEW OF WORLDWIDE REGULATORY APPROACH ON VIRTUAL CURRENCY

The more appealing features of virtual currencies are that the better-known virtual currencies, such as bitcoin, operate on the blockchain and have worldwide acceptance as an alternative payment method. Due to its convenient characteristics, virtual currencies are becoming and will continue to become a plausible method of payment and stored value for business and personal reasons, but also for criminals and terrorists. Since virtual currencies are a global currency, many countries are working on either implementing regulations to mitigate the money-laundering and terrorist-financing risks of virtual currencies, or prohibiting the use or trade of the currencies in countries like China and Ecuador.

The Financial Action Task Force (FATF), which is an inter-governmental body established with the objective of setting global standards in the form of Forty Recommendations for the prevention of money laundering and combating terrorist financing, also took action and issued publications in June 2014, Virtual Currencies – Key Definitions and Potential AML/CFT Risks, and in June 2015, Guidance for a Risk-Based Approach to Virtual Currencies. These publications provide guidance

for countries around the globe for the adoption of necessary measures for identifying potential money laundering, terrorist financing, and other crime risks associated with virtual currencies. They also emphasize in the implementation of a risk-based approach and best practices for an effective oversight of virtual currency activities to mitigate such risks.

The FATF also issued a report on July 2018, the FATF Report to G20 Finance Ministers and Central Bank Governors, identifying the different regulatory approaches being taken by a number of countries surveyed, summarized as follows:

Measures currently applied	Countries
Prohibition (on issue / use / dealing / settling of virtual currencies/crypto-assets)	China, India, Indonesia
Regulation of intermediaries / exchanges and others (using new or existing AML/CFT regulation)	Australia, France, Germany, Italy, Japan, Switzerland, US
Suspicious Transaction Reporting only	Argentina, South Africa
Preparing laws or regulations	Brazil, Canada, EU, Mexico, Netherlands, Russia, Saudi Arabia, South Korea, Spain, Turkey, UK

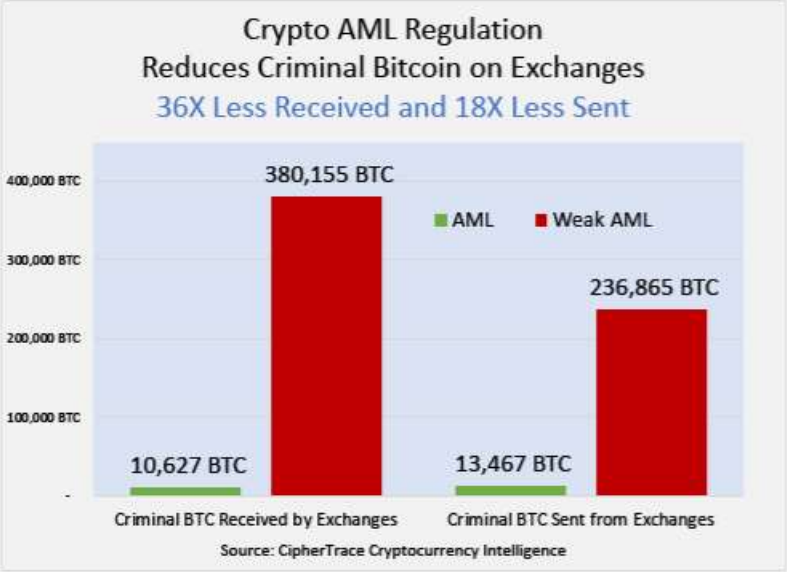
Source: *FATF Report to G20 Finance Ministers and Central Bank Governors*

In addition, FATF Executive Secretary David Lewis emphasized at the Counter-Terrorism Financing (CTF) Summit, November 8, 2018, three challenges and priorities of FATF for this year, listing virtual currencies or "virtual assets" as one of them. As he stated, "the attractiveness and use of virtual assets by criminals and terrorists has risen to the top of the political agenda."[9] For that reason, FATF revised the international standards or recommendations on October 2018 to clarify that they apply to virtual currency as well, so that "there is no excuse for countries not to act to regulate virtual assets and mitigate the risks they present". FATF expects the countries to license, register, supervise, and monitor virtual currency.

The report, *Cryptocurrency Intelligence* (2018 Q3), issued by CipherTrace, a company that provides cryptocurrency AML solutions, shows that, based on an extensive analysis of all the transactions on the top 20 cryptocurrency exchanges globally, 97% of criminal virtual currency (specifically bitcoin) that was received by global 20 (G20) top VCEs was from countries that were unregulated or posed weak AML laws. The report also indicates that 4.7% of criminal virtual currency was sent to unregulated exchanges as well.

[9] "Speech" at the Counter-Terrorism Financing Summit, November 8, 2018. http://www.fatf-gafi.org/publications/fatfgeneral/documents/speech-cft-conference-nov-2018.html. Accessed January 20, 2019.

The report further concludes that "money laundering activity using cryptocurrencies is directly correlated to AML regulations and their enforcement on exchanges...This extensive analysis shows that criminal transactions are reduced in the presence of strong AML regulations"[10] as exhibited in the graph below:



MONEY LAUNDERING CASES THROUGH VIRTUAL CURRENCY EXCHANGERS

The following money laundering cases involving VCEs highlight the importance of AML regulations and a strong AML program.

Silk Road/BitInstant

From the Department of Justice, U.S. Attorney's Office Southern District of New York: "Manhattan U.S. Attorney Announces Charges Against Bitcoin Exchangers, Including CEO of Bitcoin Exchange Company, for Scheme to Sell and Launder Over $1 Million in Bitcoins Related to Silk Road Drug Trafficking." Publication was released on January 27, 2014.

Highlights to this case relate to conspiracy to commit money laundering, operating an unlicensed money transmitter business and willful failure to file a suspicious activity report.

Bitcoin Maven

From the Department of Justice, U.S. Attorney's Office Central District of California: "'Bitcoin Maven'" Sentenced to One Year in Federal Prison in Bitcoin Money Laundering Case." Publication was released on July 9, 2018.

[10] *Cryptocurrency Anti-Money Laundering Report*, 2018 Q3, CipherTrace. https://ciphertrace.com/crypto-aml-report-2018q3.pdf. Accessed January 5, 2019.

Highlights to this case relate to operating an unlicensed bitcoin-for-cash exchange business and laundering bitcoin.

Liberty Reserve

From the Department of Justice, Office of Public Affairs: "Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million through His Digital Currency Business." Publication was released on January 29, 2016.

Highlights to this case relate to operating an unlicensed money transmitting business and helping users to conduct anonymous and untraceable illegal transactions, as well as helping to launder the proceeds of their crime. See also FATF Guidance Virtual Currency Key Definitions and AML/CFT Risks.

BTC-e

From FinCEN: "FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, DarkNet Drug Sales." Publication was released on July 27, 2017.

Highlights to this case relate to failure to obtain required customer information beyond username, password, and e-mail address, willful blindness, and offering advice on how to process and access money obtained from illegal sources. See also Prepared Remarks of FinCEN Director Kenneth A. Blanco, Delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference.

Ripple Labs Inc.

From FinCEN: "FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger." Publication was released on May 5, 2015.

Highlights to this case relate to willfully violating several requirements of the BSA by acting as an unregistered MSB, failure to implement and maintain an adequate AML program, and failing to report suspicious activity related to several financial transactions.

Common Factors That Can Be Identified Among All Cases

- Unregulated money transmitters
- Failure to establish policies and procedures for customer due diligence
- Failure to file suspicious activity reports (SARs)
- Knowingly processing transactions derived from criminal proceeds
- Willingly providing assistance to aid illicit business operations by offering advice on how to circumvent the company's policies and/or internal controls

Although in these cases only VCEs were held liable for the money laundering activity and not the banking institutions used to exchange the fiat currency to virtual currency, banks should learn from these cases and use them to strengthen their AML programs with respect to VCEs.

A financial institution may unknowingly be banking VCEs, placing the institution at higher risk of providing services to unlicensed or unregulated virtual currency businesses and laundering criminals' money. Regardless of the bank's position on banking VCEs, a bank should have controls in place to identify any and all virtual currency businesses. Depending on a bank's position, these controls should include clear policies and procedures for onboarding and handling the relationship—including risk-based due diligence and transaction monitoring, and termination of the relationship.

VIRTUAL CURRENCY EXCHANGE RELATIONSHIPS

What Are the Customer Due Diligence Obligations and Expectations for Banks Under the New FinCEN CDD Rule?

The new FinCEN Customer Due Diligence (CDD) Rule that went into effect on July 11, 2016, with full compliance date of May 11, 2018, adds on to the existing customer due diligence requirements[11] for covered financial institutions. It requires them to obtain and verify the identity of beneficial owners, who hold 25% or more of a legal entity, and the individual designated as the control person at the time an account is being opened for such entity. Although this fifth pillar of an AML program does not apply to MSBs, including VCEs, it imposes new and stringent requirements for banks.

Subsequent guidance provided by FinCEN on July 2016 and April 2018 clarifies certain aspects of the rule, such as the rule does not prohibit covered financial institutions from requesting stricter ownership percentage that the financial institution deems necessary, based on their own assessment of risk. It is also clarified that covered financial institutions are required to drill down to the ultimate beneficial owner of the legal entity. If for example, beneficial owners of a legal entity "A" are other legal entities "B" and "C," then the chain should continue until all information is collected for all natural persons that, given the percentage owned in legal entities "B" and "C," would own 25% or more of legal entity "A."

Per the CDD regulation, covered financial institutions (i.e., banks, broker-dealers, mutual funds and futures commission merchants, and introducing brokers in commodities) may rely on the

[11] "Beneficial Ownership Requirements for Legal Entity ...," *BSA/AML Examination Manual*, FFIEC. https://bsaaml.ffiec.gov/manual/RegulatoryRequirements/03. Accessed January 12, 2019.

information provided by the legal entity with regards to its beneficial owners unless the financial institution has reason to suspect inaccurate information has been provided. The regulation and guidance also provide exclusions from the definition of legal entity customers, and exemptions and limitations to such exemptions for types of accounts not covered by the new CDD Rule.

Although it is required from banks to know the ultimate beneficiary of VCEs for which they maintain accounts, banks are not expected to obtain the ultimate beneficiary of their VCE's customers. Nonetheless, banks are required to establish and implement a risk-based customer due diligence program and, based on the risk, the bank should obtain different levels of information at account opening and throughout the relationship in order to understand the nature of the business and purpose of the account being established. Sometimes the due diligence would require knowing your customer's customers, as explained further in the "What Should Banks Expect When Being Audited or Examined" section below.

What Controls Should VCEs Have in Place to Identify and Mitigate Potential Money Laundering and Terrorist Financing Risks? What Does This Mean to the Banking Institutions?

As previously stated, a regulated VCE needs to comply with all the regulatory requirements of a money transmitter. Money transmitters are not required to comply with a CIP program as banks are; however, they are required to comply with record-keeping and BSA-reporting requirements. VCEs do not have a direct or face-to-face contact with their customers; therefore, they need to take a different approach for customer identification and verification to be able to comply with regulatory requirements. Even if the VCE does not accept cash and would not be required to file currency transaction reports, they are still required to file suspicious activity reports.

Each VCE may have different requirements when onboarding a customer. Some VCEs have a set of requirements for virtual-to-virtual exchange customers and another for fiat-to-virtual exchange customers. The requirements may be as little as obtaining just an e-mail address to open or establish the account with the exchanger and as much as name, address, identification, SSN, DOB, purpose of the account, sources of funds, occupation, employment information, and so forth—just as a bank would require from its customers when opening an account[12].

Also, VCEs may have different trading limits; for instance, they may have a different trading limit for new customers than for customers who have been established for a while; or for customers who have their account linked to a credit card, compared to customers who have the account

[12] "Virtual Markets," New York State Attorney General, September 18, 2018. https://ag.ny.gov/sites/default/files/vmii_report.pdf. Accessed January 19, 2019.

linked to a bank account. Also, they may have different limits, depending on transaction types, such as wires or ACH transactions, etc.

All these factors mentioned above should be taken into consideration when making a determination on the risk the VCE may pose to the bank.

Other things to consider should be: what type of customers the VCE has; whether the VCE opens accounts for foreigners or for only U.S.-based customers; what countries the VCE customer conducts transactions with; whether they have controls in place to prevent transactions from being processed from/to sanctioned countries or jurisdictions, or from states with which they are not licensed to conduct business; what type of due diligence the VCE conducts on the exchangers they accept transfers to/from; what types of virtual currencies are traded by the VCE; whether they provide tumbler or mixing services, or have controls in place to mitigate the risk of customers transferring funds from such service providers; and whether the VCE has agents or sub-agents or bitcoin ATMs, etc.

In addition, banks should request the following information:

- ✓ Copies of all VCE required licenses and registrations
- ✓ Copy of the BSA/AML and OFAC program, and information on the VCE software used to monitor transactions for detection and reporting of unusual activity
- ✓ Copy of independent review or audit conducted by a qualified individual
- ✓ Copies of any other policies, such as fraud, complaints, identity theft, cybersecurity, privacy protection, etc.
- ✓ BSA officer background and contact information
- ✓ Description of the business operations and business projections
- ✓ Financial statements
- ✓ Flow of funds listing any other banks where the VCE maintains accounts that are expected to have transactions
- ✓ Explanation of purpose and type of activity expected for each account being opened (including number and total amount for each transaction type)

Furthermore, as part of the bank's risk-based approach, banks should also consider conducting site visits to the VCE headquarters' location.

Additionally, banks may request from the VCE to maintain a reserve account to cover the risks of financial loss in case of noncompliance.

In terms of transaction monitoring, banks can use the information provided at account opening to monitor for spikes in transactions and for comparison of actual versus expected activity. Based on the transaction review, banks may request for VCEs' financial audits, copies of reports generated by the VCEs transaction monitoring software, and conduct an analysis on where the funds are going and coming from to ensure transactions are not being conducted through dark market sites. Also, the bank can use the transaction reviews and reports produced by the VCE to identify frequent and top traders, and request copies of due diligence conducted on those traders, etc. On the other hand, banks may request access to the VCEs monitoring software and ask the VCE to provide its wallet and analyze the VCEs customer's activity themselves. However, this requires that dedicated and qualified bank personnel to conduct this type of analysis.

WHAT SHOULD BANKS EXPECT WHEN BEING AUDITED OR EXAMINED?

The FFIEC *BSA/AML Examination Manual* provides guidance on how examiners assess the adequacy of the bank's processes to mitigate risks associated with money laundering and terrorist financing. As per the FFIEC *BSA/AML Examination Manual*, banks that provide services to VCEs have the same BSA requirements and supervisory expectations as those that provide services to traditional money transmitters.

> ...An administrator or exchanger of virtual currency is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. BSA requirements and supervisory expectations for providing banking services to administrators or exchangers of virtual currencies are the same as money transmitters.
> (Refer to Nonbank Financial Institutions section of the Manual – Administrators and Exchangers of Virtual Currency)

VCEs for being money transmitters, are also categorized as nonbank financial institutions (NBFI). Banks that provide services to VCEs may be exposed to higher money-laundering risks because many NBFIs tend to fail to comply with proper licensing requirements or maintain inadequate BSA/AML compliance programs.[13] Furthermore, other risks associated with VCEs are that VCEs' entire customer base is established via non-face-to-face methods. In addition, regulations pertaining to this type of business are relatively new or are non-existent. Moreover, there is a lack of or very limited guidance on money-laundering typologies and red-flag indicators for the monitoring of VCEs' activity, although a few can be found in the *Cornerstone Report* publication on virtual currency by Homeland Security Investigations (HSI), and in an article published by

[13] "Nonbank Financial Institutions," *BSA/AML Examination Manual*, FFIEC. https://bsaaml.ffiec.gov/manual/PersonsAndEntities/04. Accessed January 12, 2019.

Reuters, "Crypto-cleansing: Strategies to fight digital currency money laundering and sanctions evasion."

Money transmitters just as any other type of customer, pose different levels of risks depending on several factors such as the type of products and services offered, locations and markets served, purpose of the account and anticipated transaction activity, etc. That being said, VCEs are likely to be classified as a higher risk type of money transmitter. The level of ongoing due diligence required to maintain the VCE relationship will depend on the risk assessment completed based on the information obtained at account opening, as discussed previously in "Virtual Currency Exchange Relationships" section. The risk assigned should also be reassessed periodically as part of the ongoing due diligence program.

The *FFIEC BSA/AML Examination Manual* provides guidance on what additional information banks may consider requiring for their higher-risk customers. Also, Risk Assessment, Risk Mitigation, and Due Diligence Expectations for Money Service Business can also be found in the *FFIEC BSA/AML Examination Manual*.

As stated in the *FFIEC BSA/AML Examination Manual*, banks are not expected to be the regulators of VCEs, however, banks are expected to establish and implement a risk-based compliance program. They are expected to implement controls and due diligence processes to mitigate the risks associated with banking VCEs. To that end, banks should expect that auditors and regulators would be evaluating the factors that were taken into consideration to assess the risk exposure and, based on that evaluation, would be evaluating the intensity of the due diligence that banks conducted on their VCE customers to mitigate those risks.

Regulatory Expectations

The following regulatory expectations apply to banks with MSB customers as outlined in the FFIEC Manual[14]:

- The BSA does not require, and neither does the FinCEN nor the federal banking agencies expect, banks to serve as the de facto regulator of any type of NBFI industry or individual NBFI customer, including MSBs.
- While banks are expected to manage risk associated with all accounts, including MSB accounts, banks will not be held responsible for the MSB's BSA/AML program.

[14] "Nonbank Financial Institutions," *BSA/AML Examination Manual*, FFIEC. https://bsaaml.ffiec.gov/manual/PersonsAndEntities/04. Accessed January 12, 2019.

- Not all MSBs pose the same level of risk, and not all MSBs will require the same level of due diligence. Accordingly, if a bank's assessment of the risks of a particular MSB relationship indicates a lower risk of money laundering or other illicit activity, a bank is not routinely expected to perform further due diligence (such as reviewing information about an MSB's BSA/AML program) beyond the minimum due diligence expectations. Unless indicated by the risk assessment of the MSB, banks are not expected to routinely review an MSB BSA/AML program.
  (Refer to Nonbank Financial Institutions section of the Manual – Regulatory Expectations)

WHAT RESOURCES ARE AVAILABLE TO BANKS TO MITIGATE THE RISKS THAT ARE POSED BY BANKING VIRTUAL CURRENCY MSBs?

"Knowledge Is Power"

Below is a list of resources that, while conducting my research, I found them to be good source of information.

- ➔ FATF Guidance for a Risk-Based Approach to Virtual Currencies
- ➔ The FATF Recommendations – Revised October 2018
- ➔ FinCEN Customer Due Diligence Requirements for Financial Institutions; Final Rule
- ➔ DFS – Information and Resources for Virtual Currency Business Activity (BitLicense)
- ➔ Commodity Futures Trading Commission (CFTC) Virtual Currency Resource web page
- ➔ FFIEC Examination Manual
- ➔ United Nations Office of Drugs and Crime (UNODC) – Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies
- ➔ Nationwide Multistate Licensing System
- ➔ Report issued by the Office of the New York State Attorney General, Barbara D. Underwood titled Virtual Markets Integrity Initiative, which explains to consumers and investors how VCEs "operate, protect consumer funds, and ensure the integrity of transactions."
- ➔ J.P. Morgan Perspectives – Decrypting Cryptocurrencies: Technology, Applications and Challenges

In addition to resources readily available regarding Virtual Currency Exchanges, such as the ones previously mentioned, regulators and subject matter experts would continue to issue guidance and best practices as the industry matures. Websites from various anti-money laundering associations frequently post publications on different areas related to virtual currency and other topics as well.

CONCLUSION

While conducting this research on virtual currency exchangers, I found it to be shocking, although expected given that regulations are still being enforced worldwide, that certain states have not issued guidance on whether VCEs are even required to be licensed at the state level, much less on how to approach virtual currency exchange relationships. There is an extensive list of resources available to read on virtual currencies and the technology itself, however, there is minimum to no guidance on how banks can monitor their VCE transactions for unusual activity.

What is left then? While FinCEN, the banking regulators, and law enforcement agencies build up on data to study the trends and come up with additional guidance on suspicious activity and red-flag indicators, banks must heavily weigh the customer due diligence requirements to establish and monitor VCE relationships. Certain risks associated with VCE relationships, as discussed throughout the document, may be mitigated by establishing a close relationship with their VCE customers as well as by continuous monitoring.

Understanding of the VCE's customer base and the VCE KYC program is key for a thorough evaluation of the VCE risk exposure to the bank and for a satisfactory rating in a BSA/AML audit or examination.

REFERENCES

CipherTrace Cryptocurrency Intelligence. (2018, Q3). *Cryptocurrency anti-money laundering report*. CipherTrace. Retrieved from https://ciphertrace.com/crypto-aml-report-2018q3.pdf

Department of Financial Services. (n.d.) Virtual currency businesses. New York State. Retrieved from https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses

Divisions of Corporate Finance, Investment Management, and Trading and Markets. (2018, November 16). Statement on digital asset securities issuance and trading. U.S. Commodity Futures Trading Commission. Retrieved from https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading

Divisions of Enforcement and Trading and Markets. (2018, March 7). Statement on potentially unlawful online platforms for trading digital assets. U.S. Securities and Exchange Commission. Retrieved from https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading

FFIEC BSA/AML Infobase. (2018). Beneficial ownership requirements for legal entity customers—Overview. *BSA/AML Manual.* Retrieved from https://bsaaml.ffiec.gov/manual/RegulatoryRequirements/03

FFIEC BSA/AML Infobase. (n.d.). Nonbank financial institutions—Overview. *BSA/AML Manual*. Retrieved from https://bsaaml.ffiec.gov/manual/PersonsAndEntities/04

FinCEN. Guidance on existing AML program rule compliance obligations for MSB principals with respect to agent monitoring. (2016, March 11). U.S. Department of the Treasury. Retrieved from https://www.fincen.gov/resources/statutes-regulations/guidance/guidance-existing-aml-program-rule-compliance-obligations

FINRA. (2019). State securities regulators. Retrieved from http://www.finra.org/investors/state-securities-regulators

Lewis, D. (2018, November 8). Speech at the counter-terrorism financing summit, Bangkok. FATF. Retrieved from http://www.fatf-gafi.org/publications/fatfgeneral/documents/speech-cft-conference-nov-2018.html

Office of Customer Service and Outreach. (2018, March 17). An introduction to virtual currency. U.S. Commodity Futures Trading Commission. Retrieved from https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/oceo_aivc0218.pdf

Office of the New York State Attorney General. (2018, September 18). *Virtual markets integrity initiative report*. Retrieved from https://ag.ny.gov/sites/default/files/vmii_report.pdf

U.S. Commodity Futures Trading Commission. (2018, May 21). CFTC staff issues advisory for virtual currency products. Retrieved from https://www.cftc.gov/PressRoom/PressReleases/7731-18

U.S. Securities and Exchange Commission. (2009, January 30). Alternative trading system (ATS) list. Retrieved from https://www.sec.gov/foia/docs/atslist.htm

APPENDICES

Acknowledgements

I would like to use this section to acknowledge (in alphabetical order) the following individuals for their expert contribution to this whitepaper.

Andrew Grammatikos – IRS Special Agent

Asif Sardar, CAMS, CFE – Director, Regulatory Risk Practice, Protiviti

David Landsman – formerly Executive Director of the National Money Transmitters Association (NMTA), now Principal at David Landsman Consulting, LLC, where he offers AML consulting services.

Jeremy Rosenberg – Supervising Investigator, New York District Attorney's Office, Homeland Security Investigations (HSI) / El Dorado Task Force – High-Intensity Financial Crimes Area (HIFCA)

Ross S. Delston – Attorney and Expert Witness, former U.S. Banking Regulator (FDIC)

Ruben Sanchez, Sr. – President and CEO, BSA Compliance Solutions – Expert in matters concerning cryptocurrency and high-risk financial services.

About the Author

Mariel Diaz is a certified anti-money laundering specialist (CAMS) with over 15 years of experience in the BSA/AML field. She is currently the AML Quality Control Officer of a New York based bank where she transitioned from her AML transaction monitoring manager role. Prior to serving the banking industry, she was the Chief Compliance Officer of a money transmitter company, also headquartered in New York. Her experience extends from financial crimes investigations to the development and administration of a comprehensive compliance program, inclusive of transaction monitoring system implementation, validation and maintenance, customer due diligence and enhanced due diligence programs, and AML quality control program development and implementation. She has worked closely with senior management in risk assessments, independent audits, and regulatory examinations.

Her professional affiliations include the Association of Anti-Money Laundering Specialists (ACAMS), ACAMS New York Chapter, and the American Bankers Association (ABA).