Top 15 Frequently Asked Questions on Cryptocurrency for Financial Crime Prevention Professionals

Our series with CipherTrace, ***Digital Currencies: Understanding Expectations and Managing Your Risk*****,** took place recently and piqued our audience's interest, sparking many questions. We're happy to share the top FAQs from the session to help your financial institution better understand cryptocurrency and how it affects your organization.

Catch up on the insight series here!

1. Why do all banks have crypto exposure?

People seem to think that not all banks are linked to crypto activity because they don't all directly provide cryptocurrency services, but in reality, the risk crypto presents is everywhere. Extensive research by our partner, CipherTrace, uncovered that individuals are operating illicit crypto Money Service Businesses (MSBs) at eight out of every 10 U.S. retail banks. These illegal MSBs use their demand deposit accounts (DDA) as a conduit for the illegal trade of fiat for crypto by accepting cash payments in exchange for cryptocurrency. They often do this with a simple ACH transfer, wire transfer, or counter cash deposit at a depository institution. Peer-to-peer (P2P) crypto marketplaces also exist specifically designed to help people buy and sell cryptocurrencies using in-branch cash deposits or discrete wire transfers. To conceal the use of unregistered MSBs, buyers are often told not to inform bank tellers that they are making deposits to purchase bitcoin but rather tell them they are purchasing "digital services." Because illegal MSBs and P2P crypto marketplaces constantly leverage the banking system, even banks not looking to onboard or bank Virtual Asset Service Providers (VASPs) must be able to understand and identify their crypto risk exposure.

2. What risk do Peer-to-Peer (P2P) exchanges pose to financial institutions? What tips do you have on how to detect the activity of unregistered P2P exchanges within bank deposit account activity?

P2P exchanges create exposure for banks because many are unlicensed MSBs. An unlicensed or unregulated business creates a sizeable risk for any financial service organization doing business with them, including the significant risk that the unregistered/unregulated organization has insufficient controls, or doesn't care whether or not they are transacting with criminals. Meaning any financial services organization (FSO) doing business with them is potentially facilitating money laundering. Continuous monitoring of P2P sites and dark markets is crucial for detecting P2P exchanges. To detect P2P activity in a bank deposit account, both the inflows and outflows of funds for that specific account need to be monitored. You also need to monitor the risk of each transaction source and destination and monitor for typologies such as structuring and burst transactions that can be good indicators of suspicious P2P activity. Using

intelligence obtained from CipherTrace data, NICE Actimize detection will identify and alert users to suspected P2P crypto exchanges.

3. If a customer uses their account for crypto transactions but the account was not opened for that purpose, can transaction monitoring identify the crypto transactions?

Advanced transaction monitoring can identify payments to and from VASPs based on true names, DBAs and bank accounts.

4. How much comfort can a financial institution get from AML procedures/policies at 'regulated' exchanges? What else can be done to increase the level of comfort at inception and ongoing?

Financial institutions should take comfort in the growing regulation of the industry and proposed regulation of Novel Institutions in the U.S. There are also tighter regulations in Europe in the form of the 5th Money Laundering Directive. These regulations and recent case laws make trading with regulated exchanges safer for all customers and financial institutions. In March 2021, the Commodity Futures Trading Commission (CFCT) issued an order filing and settling charges (including a $6.5 million settlement) against a cryptocurrency exchange for "reckless, false, misleading, or inaccurate reporting as well as wash trading" on its GDAX platform. Other leading cryptocurrency exchanges have been investigated for their trading practices, as well. Recently, the UK FCA announced that they were extending their temporary register regime while working through the significant number of applications from VASPs. The FCA disclosed that several VASPs were not meeting AML regulatory standards, and as a result, a number withdrew their applications and ceased trading. This FCA enforcement shows that digital currency organizations have to meet the expected standards or fall on the wrong side of regulatory enforcement.

There is obviously still more to be done as not all countries regulate VASPs. To protect your organization, you must have a technology solution that can understand the risk associated with each VASP and have a way of monitoring your customers' activity for suspicious transactions.

5. For any bank that does not onboard VASPs and has no direct crypto activity, what are the minimum actions it should be doing?

Banks need to be asking themselves the following questions:

- What baseline controls do we have in place to identify customers dealing with virtual assets?
- Do we have institutional or peer-to-peer virtual currency customers?
- How does our financial institution interact with emerging payment systems?
- Do we have the tools we need to identify and report potentially suspicious activity occurring through our financial institution?

All these questions impact the policies and procedures banks need to put in place to mitigate risk. If banks are not thinking about these issues, it introduces risk to their system and will be apparent when examiners visit. Kenneth Blanco, the Director of the Financial Crimes Enforcement Network, touched on this during his address at a recent

ACAMS conference: *"To be clear, exchanges are not the only ones with crypto risk exposure. These risks are not unique to money services businesses or virtual currency exchangers; banks must be thinking about their crypto exposure as well. These are areas your examiners, and FinCEN, will ask you about when assessing the effectiveness of your AML program."*

At a minimum, to manage risk, banks need the tools to understand the risk of a VASP and have visibility to which, if any, of their customers are transacting with a VASP, especially a VASP considered to be high risk.

6. Any suggestions for financial regulators to help U.S. banks understand this risk, other than FATF references?

The plethora of headlines over cyberattacks and ransomware attacks, as well as the proposed changes to banking regulations in the U.S. for "Novel Institutions," are growing. These articles contain a wealth of information to help identify and mitigate risk exposure. There are also new crypto regulations at the state level, which regulatory agencies will heavily enforce. Reading the FATF website and FinCEN proposals and subscribing to the CipherTrace newsletter and blog are good ways for both regulators and financial institutions to keep up with changes.

7. Are Decentralized Finance (DeFis) exempt from AML and KYC controls?

We expect clarification to include decentralized cryptocurrency exchanges (DEXs).

8. How can a truly DeFi system be monitored by a government as far as BSA/AML, etc.? Only on the on/off ramps, perhaps?

Correct, just like with centralized exchanges, the on/off ramps are the choke points where effective monitoring can be used to help identify BSA/AML suspicious activity.

9. Are there official lists with registered and non-registered VASPs?

FinCEN has a list of registered MSBs, but does not explicitly identify VASPs. Outside the U.S., other regulators such as the FCA in the U.K. and BaFin in Germany also maintain lists of regulated organizations, but do not maintain lists of non-registered MSBs and VASPs. CipherTrace tracks non-registered VASPs and exposes that data through NICE Actimize solutions.

10. Is there a website we can check to see if a VASP is being regulated?

Not yet; CipherTrace does identify which jurisdiction a VASP operates in—helping organizations determine whether or not the VASP is in a high-risk jurisdiction or a jurisdiction with little or no regulatory oversight.

11. What happens when a sanctioned address uses mixing services to send coins to millions of random addresses to taint everyone?

This is identified through the monitoring provided in the joint NICE Actimize and CipherTrace solution. By looking back at the hops when monitored at the receiving financial institution, the transaction(s) will be flagged as a high-risk transaction. An investigator can then review the information presented to them to make a disposition decision on the alert.

12. In which country are the most crypto assets mined?

The Nordics top the list of countries with the most activity. You can reference this list to see the top countries mining crypto.

13. If blockchain analysis can be done and can identify the person(s) behind a cryptocurrency transaction, does that make the whole anonymity of crypto a myth?

Crypto, specifically Bitcoin, has never been anonymous. They are typically classified as pseudonymous due to the publicly available ledger (the blockchain) that tracks all transactions and balances. U.S. courts have ruled that there is no expectation of privacy for individuals who use a public ledger cryptocurrency.

14. What are privacy coins, and how risky are they?

Privacy coins are a type of cryptocurrency that obscure each coin transaction's source and end destination. These coins are said to provide privacy to owners and receivers by protecting their information. More well-known privacy coins include Monero and Dash. Privacy coins introduce risk into the financial system because the privacy they provide could allow for money laundering and counter-terrorist financing (CTF). Due to this, privacy coins have been delisted from several exchanges and have varying levels of legality depending on the jurisdiction you are in. FATF recently published draft guidance that states, *"If [a] VASP cannot manage and mitigate the risks posed by engaging in [activities that involve the use of anonymity-enhancing technologies or mechanisms], then the VASP should not be permitted to engage in such activities."*

15. How many crypto assets are used for illicit purposes, and what is the trend?

According to lawyer Hailey Lennon, who was regulatory counsel for cryptocurrency platforms Coinbase and bitFlyer, a *"false narrative about cryptocurrency transactions has been created."* The majority of cryptocurrency is not used for criminal activity. That being said, there is evidence that cryptocurrencies are used for illicit activity and are used as a means to launder illicit wealth around the globe; you only need to read recent media articles about law enforcement seizing millions of dollars worth of cryptocurrencies from criminals. It is globally recognized that virtual assets are not as extensively used for illicit purposes as fiat currency. However, all financial service organizations need to have appropriate and effective monitoring in place to identify those transactions that are suspicious.

For additional information, please visit our website or contact us at AskTheExperts@niceactimize.com.