Being an AML Detective in the Crypto World!

Do you want to be a successful AML detective in the cryptocurrency world? Come on, who doesn't!! Most people think "crypto" and they get scared.

Why? Because people fear the unknown. Yes, it's still in its infancy, but it's not like it was created this year. Believe it or not, crypto started around 10 years ago.

Crazy, right?? And it's developing into a bigger and bigger market. It's even considered an asset class now. Who knows, it might replace the dollar one day. In my opinion, I think it will.

So, with the future of crypto being bright, it's important that we, as AML detectives, understand all the different aspects. Remember, knowledge is power!!

To start, how much does the typical person understand about the crypto world. In order to get over the fear of cryptocurrency, we need to understand. Unfortunately, we can't tell criminals that in the compliance world compliance professionals are fearful. They would probably laugh just like I'm doing now.

For criminals, to commit a crime, fear doesn't come into the equation. Criminals always try to create new opportunities in new and upcoming markets. Think of them as entrepreneurs, I guess.

So, let's start out by defining cryptocurrency; Let's look at a quick definition by *Wikipedia* (my favorite source):

A cryptocurrency, crypto-currency, or crypto is a collection of binary data which is designed to work as a medium of exchange. Individual coin ownership records are stored in a digital ledger, which is a computerized database using strong cryptography to secure transaction records, control the creation of additional coins, and verify the transfer of coin ownership. Cryptocurrencies are generally fiat currencies, as they are not backed by or convertible into commodities. Some crypto schemes use validators to maintain the cryptocurrency.

A cryptocurrency is a tradable digital asset or digital form of money, built on blockchain technology that only exists online. Cryptocurrencies use encryption to authenticate and protect transactions, hence their name. There are currently over a thousand different cryptocurrencies in the world, and their supporters see them as the key to a fairer future economy.

Since we got the semantics out of the way, let's dive into how money launderers use cryptocurrency to launder money. In the AML world, launderers go through the same three stages to clean money as they do with crypto, with some differences.

- First is the **Placement** stage. In this stage, money launderers convert their dirty money or illegal gains into cryptocurrency. We are talking about criminal activity that involves drugs, terrorist financing….
- The second stage is **Layering**. For layering, you obviously want to make it tough to trace. If it's channeled between different wallets the audit trail becomes more obscure. Then, the criminal funds are co-mingled with legitimate funds to make it difficult for anyone, particularly law enforcement, to track and identify.

- The final stage is **Integration**. The now co-mingled funds, illegal and legal funds, are then converted back to cash or used to purchase any type of goods or services. Criminals can purchase cars, homes, fine art..

This whole process can take days, weeks, or months to accomplish. In the end, this is how revenue generated through illegal activity is incorporated into the financial system. It might be time-consuming for a criminal, but the goal is to have funds, so they look like the average citizen.

Money laundering Schemes

Did you ever ask yourself what type of schemes money launderers use? I find it interesting but also very educational. As technology has advanced, criminals are also using it to their advantage. Since the creation of cryptocurrency, the opportunities for money launderers have only increased. I searched the internet to find different ways criminals launder money. Obviously, there are many schemes, new and old.

Remember, you are an AML Detective and must be an expert in spotting these. Here are some of them:

- Setting up a cash-intensive business such as restaurant, laundry mat, car wash, strip club, supermarket, car service.
- Structuring (or Smurfing). Structuring has been around forever. This is when someone takes an amount of illegal funds and breaks it into smaller amounts in order to make it less suspicious using money orders, cashier's checks. Then they are deposited into accounts.
- Creation of shell companies. They do not have any business operations or anything else active. The sole purpose is to hide money.
- Trusts are used to conceal ownership information.
- Trade-based laundering involves altering invoices or business documents to disguise dirty money as business profits.
- Bank Capture is when the money launderers run a financial institution. This way, money can move to different financial institutions without raising any red flags since the operational component can be hidden by the higher-ups.
- Casino laundering. To me, this is the easiest. Maybe because I have visited casinos in my day and see how it can be done. Casino chips can be purchased, maybe gambled a little, then turned back into cash and be claimed as gambling winnings.
- Real Estate can be purchased with cash and then sold quickly. This is completely legal. Also, criminals can potentially make a profit from their illegal gains. Suspicion could be raised if it's done too often.

My goal with providing money laundering schemes is not to give you ideas on how to do it, but as AML detectives, we need to understand the various ways criminals try to circumvent the system. Plus, maybe I have seen too many movies based on these schemes, but it is interesting.

Now it's time to start digging into the regulatory weeds. It's really important to understand the foundational elements and then build upon them while staying on top of the news for changes. You can't put it down for 6 months and then pick it up again and be an expert. Do you want to be an AML detective?

Let's start by discussing the AML risks with cryptocurrency…

Cryptocurrencies are known for transactions that are conducted between two different individuals or entities. This keeps certain institutions and authorities (domestic and global) out of the way. This allows people to be free and clear to conduct their transactions as they wish.

Criminals know that this information and they try to use cryptocurrency to send illegally gotten gains across the globe. As AML detectives, we have to understand the differences between using cryptocurrencies and traditional finance. They are different.

From the internal side, we can conduct the typical KYC process, monitoring and leveraging other tools to try and identify the criminal elements and stop them in their tracks. But who oversees from a regulatory perspective? We need to look at the Financial Action Task Force (FATF) – the global money laundering and terrorist financing watchdog.

The FATF conducts a lot of research in virtual currencies to understand the current environment. They know that this new class of assets poses risks to everyone involved, even the criminal element. Based on the risks to the financial system, the FATF came out with a report that lists the most relevant risks. They include:

- The anonymity offered by virtual assets on the internet.
- The limited scope of the user verification and identification process.
- Gaps in understanding, supervising, enforcing, and complying with the AML/CFT standards for cross-border. cryptocurrency transactions.
- The absence of a body to oversee and ensure compliance.

This list addresses some of the concerns and risks with cryptocurrencies, but there are more of course. Let's now examine the type of AML red flags that can be present.

AML Red Flags

As AML detectives, we need to identify the red flags that I've learned in life not to make assumptions. If you break it down it means to make an ass out of you and me! So, with that out of the way, let's define what is a red flag? I like this definition courtesy of BitAML:

Red flags are hypothetical scenarios that could indicate suspicious activity in transactions. Basically, they are a series of thresholds that tell you "if a transaction looks like this, it might be suspicious."

Since red flags enable you to identify potentially illicit activity, they will form the basis of your surveillance and monitoring policy. A strong policy will include the red flags unique to your institution in detail, giving your employees a list to refer to as they monitor transactions.

Essentially, if something doesn't seem right or smell right, that needs to be investigated. As an AML Detective, it is our duty and responsibility to look into anything that doesn't pass the smell test. And if an investigation is needed, then the proper escalation needs to occur.

The risks for not investigating pose the firm to legal, financial, reputational, and other types of risk. I wouldn't want that in my head if something that needed to be researched didn't occur.

Crypto laundering mimics similar steps to cash money laundering which are firstly Placement, then Layering and finally Integration

Placement

Firstly, criminals convert cash into cryptocurrency.

Layering

To layer the cryptocurrency and make it difficult to trace, it is channeled between wallets or through "tumbling/mixing services".

Integration

The illegal cryptocurrencies are then converted back to cash or are used to purchase goods or services.

In order to identify reg flags, we need to be as educated as possible. Luckily, the FATF provides us with a lot of details based on the research they conduct. To reiterate, the FATF combats money laundering on an international stage. Why am I bringing this up now? Because the FATF published money laundering red flag indicator guidelines to provide cryptocurrency exchanges with detailed information for minimizing crypto-related AML risks

We also must look at other issues in catching these criminal elements and determining potential red flags. The real issue is how they protect their investments.

Criminals who use crypto wallets make it almost impossible for anyone, particularly a regulator, to access or move those funds without the wallet's private key. A lot of investors use hardware wallets to protect their investments from theft or access by regulators.

With any type of criminal, in particular Money launderers, they attempt to find loopholes by moving their funds to platforms in other jurisdictions, where AML compliance isn't as enforced as other jurisdictions. So, we need to look at the particulars in determining whether there is a red flag or if the person is a legitimate person who uses a cryptocurrency account for investment purposes.

Here are four prevalent money laundering schemes that can be found in the crypto industry today.

1. **Tumbling/Mixing Services**: In this scheme, a service is offered to criminals whereby they are allowed to mix suspicious cryptocurrency funds with other funds, making the illegal coin trail hard to trace by auditors.
2. **Unregulated Exchanges**: To avoid coming into the spotlight while cleaning their dirty funds, criminals often opt to transact through unregulated cryptocurrency exchanges. Such platforms have inadequate AML procedures in place, making it easy for money launderers to cover their tracks. Without any transaction monitoring or background screening process, illegal funds are left unnoticed. This scheme was used in 2018 during the famous 2018 Coincheck money laundering scandal.
3. **Online Casinos:** Laundering cryptocurrency through an online casino is a fairly simple scheme. Criminals place their bets through stolen coins. Once the game is finished, the winning coins are withdrawn and

exchanged for real money. While this does not allow them to launder huge amounts, legitimate money is received in the end.

4. **Money Mules**: Fraudsters often recruit money mules, i.e., individuals with clean transaction history, to launder illicitly earned cryptocurrencies. In some cases, criminals use Ponzi schemes to collect bitcoins from victims and money mules transfer the coins between accounts to hide the source of the illegal coins. According to Europol, 90% of all money mule transactions in Europe are connected to cybercrimes.

So, if we are looking for red flags, yes, we must look at their transactions, other activities, but also have to look at their residence, nationality, and occupation. When we put this all together, we are essentially building a case to determine whether the situation is a red flag or not.

As AML detectives, we can't let the simplest little item to pass without doing a thorough investigation. Remember, we are detectives and as such, we need to look at everything. If we don't, think of the consequences of our actions or inactions.

To stay clear of money laundering and similar financial crimes, cryptocurrency exchanges must have adequate AML checks and KYC procedures in place.

These practices have not only been endorsed by global regulatory authorities but have shown encouraging results in the real world as well. As cryptocurrency adoption is showing no signs of slowing down, firms must invest in the right AML solutions to streamline compliance and fraud detection processes.

Hopefully, this provides you with a taste of what to look for, how to look for it, and what to consider during your research. As AML detectives, we need to educate ourselves to understand the types of red flags, where they originate from, and what to do about them. Good luck!!

Sources:

- What is AML in Crypto: Track Suspicious Transactions - Phemex Academy
- Sign up - Coinbase
- AML Regulations and Cryptocurrency Businesses | sanctions.io
- Money Laundering Through Cryptocurrency: Red Flags and AML Risks (shuftipro.com)
- Cryptocurrency Transaction Monitoring: Adapting AML | Quantexa
- Cryptocurrency Anti-Money Laundering AML Risks & Regulations | TTI (truthtechnologies.com)