TRM

Compliance in the second age of digital assets

How crypto compliance programs are evolving

trmlabs.com

Introduction

Around the same time that Silicon Valley Bank, lender to some of the world's leading startups, entered receivership on March 11th, 2023, US regulators also shuttered two smaller institutions: Signature Bank and Silvergate Bank.

Despite their lack of big name recognition, Signature and Silvergate provided a unique service for crypto clients: their blockchain systems allowed instant commercial transfers in and out of crypto around the clock, enabling over 2 trillion US Dollars to be moved to and from digital asset markets since 2019.

According to Bloomberg, Department of Justice (DOJ) investigators had been examining whether Signature took sufficient steps to detect potential money laundering by clients through Know Your Customer (KYC) checks and transaction monitoring. Meanwhile, Silvergate is facing a DOJ fraud probe over its dealings with the collapsed cryptocurrency FTX and its sister company Alameda Research.

Whether or not either bank will be found to have committed any wrongdoing, their abrupt demise and associated regulatory scrutiny exposes urgent compliance challenges facing institutions that have connectivity with crypto. Regulators in the U.S. and abroad have clearly signaled in the early months of 2023 that the expectations for risk management and crypto are high.

The first age of risk management in digital assets was a patchwork approach, primarily driven by law enforcement prosecutions of bad actors and global regulators grappling with traditional anti-money laundering, securities and consumer protection laws applied to new assets and activities.

The Second Age of Digital Assets will be heavily influenced by three key themes:

The adjustment of historical compliance frameworks to a decentralized world

The rise of supervisory transparency

The transition from technical compliance to effectiveness

TABLE OF CONTENTS

Adjusting historical compliance frameworks to reflect a decentralized world

The increased use of cryptocurrency in finance has fundamentally altered the central object of compliance frameworks. Because banks and money services businesses have historically monopolized financial flows, it made sense for AML legislation to be targeted at these traditional gatekeepers.

Today's digital asset ecosystem remains reliant on such legacy intermediaries to provide cash-out points, on and off-ramps and fiat capital allocation to fuel growth.

Yet the rise of automated market makers, peer-to-peer networks, and transactional activity run exclusively by software code has eroded the monopoly of traditional financial institutions over transaction execution. What are the regulatory implications of this emerging ecosystem — and what does this mean for compliance programs both within decentralized economies and those traditional institutions who will be a counterparty to it?

Back in 2020, Jai Ramaswamy, former U.S. Department of Justice Section Chief of Asset Forfeiture and Money Laundering and current Chief Legal Officer at Andreesen Horowtiz, wrote a prescient piece titled *"How I Learned to Stop Worrying and Love Unhosted Wallets."* It described the rising regulatory tension between traditional compliance frameworks and a new digital asset infrastructure built on distributed ledger technology.

Ramaswamy posited that the rise of private stablecoins and decentralized finance networks may shift regulatory priorities and perceptions around issues like AML enforcement. Many of the headline events of 2022 have seemingly brought that issue to the fore. Indeed, we see regulators increasingly focus on specific nexus points of illegal or illicit activity, irrespective of where that point sits on the spectrum between fully decentralized and fully centralized.

OFAC's decision to designate Tornado Cash appears to reflect this new thinking. While the US authorities had long called out crypto mixers as a threat and potential target for enforcement, the designation itself was a watershed moment in regulation as it effectively sanctioned a smart contract or code. Similarly, the US Commodity Futures Trading Commission (CFTC) brought a civil enforcement action against Ooki DAO, a decentralized autonomous organization. And in the final days of 2022, Avraham Eisenberg, a crypto trader allegedly responsible for draining a DeFi trading platform called Mango Markets to the tune of $110 million, was arrested by US authorities for allegedly manipulating a decentralized-finance trading platform which operated as an automated market maker.

TABLE OF CONTENTS

Introduction

Designing an effective AML program

Conclusion

In April of 2023, the United States Treasury Department released its Illicit Finance Risk Assessment of Decentralized Finance (the "assessment"). The report on DeFi notes that AML obligations in the U.S. are activity-based, and asserts that the BSA requires entities acting like financial institutions to "establish and implement an effective anti-money laundering program," and comply with OFAC sanctions.

Multinational bodies such as FATF and the EU continue to grapple with the CeFi/DeFi binary and how to adequately assess true decentralized infrastructure projects from those carrying the "decentralized" name but share features of CeFi. For example, while FATF standards do not apply to software such as DeFi protocols themselves, they can apply to persons who maintain control or sufficient influence over a DeFi arrangement or protocol providing VASP services.

Similarly, although DeFi currently falls outside the EU's Market in Crypto-Assets (MiCA) legislation, individual entities could potentially be answerable to the Fifth Anti-Money Laundering Directive (5AMLD) if a supervisor identified a "person with significant control" that should be registered as a cryptoasset service provider due to the services the DAO is carrying out.

These issues present complex legal questions where we will see significant enforcement variation between jurisdictions. What remains clear is the growing importance of how risk management will coexist within principles of decentralization.

Such moves mirror similar practices taking shape within the industry. For instance, DeFi protocols such as Uniswap — one of the leading decentralized crypto exchanges executing automated order book trading — look to comply with sanctions requirements by implementing automated sanctions screening. Utilizing blockchain intelligence tools via APIs, Uniswap is able to query data about on-chain addresses or transactions to detect sanctions exposure and receive risk indicators back that can be used to block addresses from interacting within the protocol through its front-end website. **Moreover, the visibility of blockchain data allows organizations to surface this sanctions risk even where it may be obfuscated or attenuated (see image 1).**

Without large compliance departments, the process enables the detection and prevention of illicit finance entering the financial ecosystem, which is at the heart of any AML program. It is these types of processes and experimentation that can form the building blocks for how to build and scale risk management solutions as the surface area of decentralization expands.

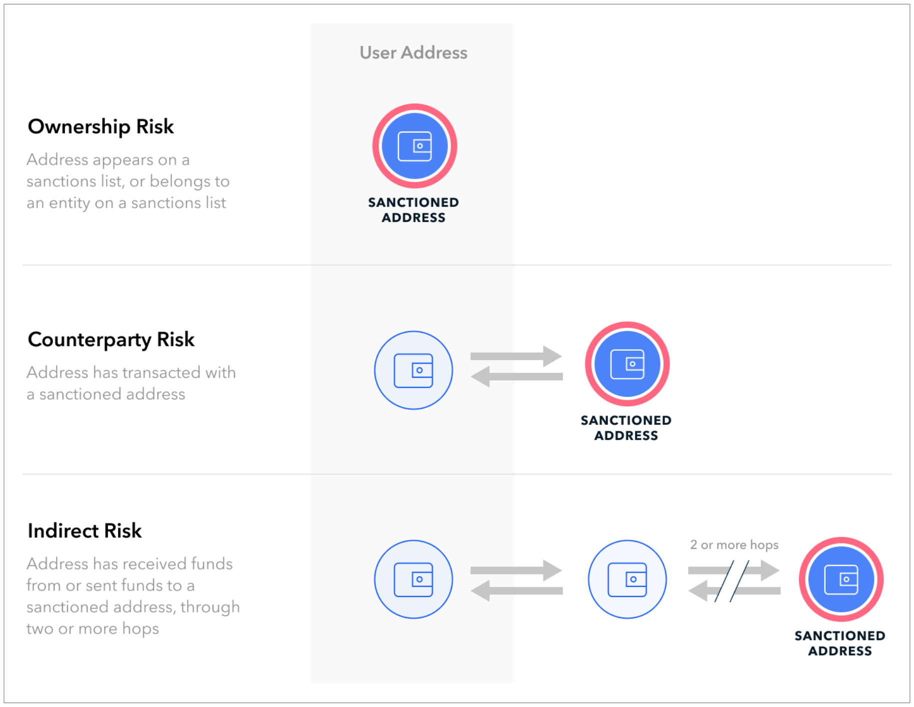

User Address
Ownership Risk
Address appears on a sanctions list, or belongs to an entity on a sanctions list
SANCTIONED ADDRESS
Counterparty Risk
Address has transacted with a sanctioned address
SANCTIONED ADDRESS
Indirect Risk
Address has received funds from or sent funds to a sanctioned address, through two or more hops
2 or more hops
SANCTIONED ADDRESS

Image 1. On-chain risk types for sanctions

The evolution of blockchain intelligence for supervisory awareness

Regulatory pressure from policymakers on crypto companies is increasing. Yet a potentially even larger impact on the industry may result from supervisory bodies, and their own implementation of blockchain analytics tools.

When regulators currently review AML programs in their respective jurisdictions, are they sampling the group of transactions and customers most salient to the institution's actual level of risk? How do they know whether the institution has adequately captured all relevant risks in their risk assessment (as opposed to only the risks the institution is aware of)?

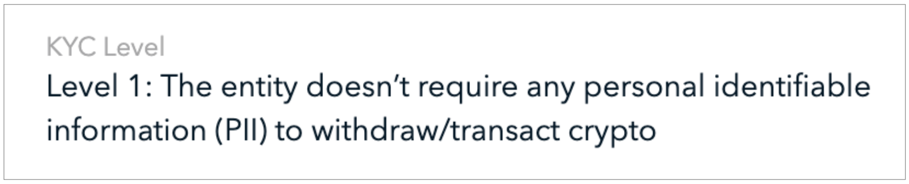
At present, much of their review involves evaluating policies and procedures, risk assessments, sampled alerts and customer risk profiles. In this process, there can be an element of blind sampling and trust in what's on paper.

Blockchain intelligence can improve this process by arming regulators with a level of transactional risk transparency not previously available. Consider a hypothetical scenario in which a regulator examines an institution with a similar on-chain profile to Bitzlato, the Hong Kong-registered cryptocurrency

TABLE OF CONTENTS

exchange recently identified by FinCEN as a primary money laundering concern for its connection with Russian illicit finance.

Blockchain intelligence could reveal a number of material, risk relevant data points that are not apparent from policies, procedures or alert samples. For instance, the regulator might observe that despite it purporting to do KYC, test accounts and transactions with the exchange reveal that the institution in fact collects no documentation whatsoever at onboarding.

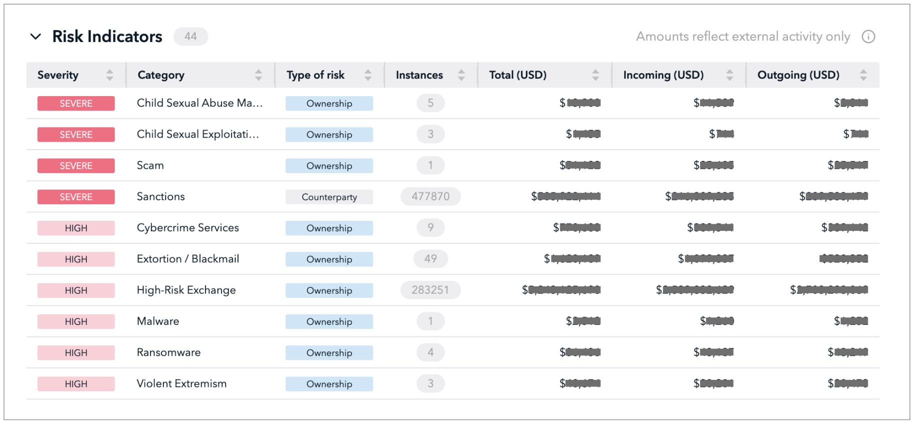


KYC Level

Level 1: The entity doesn't require any personal identifiable information (PII) to withdraw/transact crypto

Image 2. KYC Levels can serve as an indicator for how much documentation an entity actually collects at onboarding, irrespective of written policies

If the regulator wanted to sample transactional activity, blockchain intelligence can give it the ability to begin its review with transactions that carry the most severe risk, with counterparties directly connected to ransomware, scams, darknet markets or other cybercrime services. Moreover, the regulator could ascertain whether those high risk transactions represent a systemic facilitation of illicit activity indicative of control failures, or are merely one-off instances.



Risk Indicators 44

Amounts reflect external activity only

Severity	Category	Type of risk	Instances	Total (USD)	Incoming (USD)	Outgoing (USD)
SEVERE	Child Sexual Abuse Ma...	Ownership	5	$[redacted]	$[redacted]	$[redacted]
SEVERE	Child Sexual Exploitati...	Ownership	3	$[redacted]	$[redacted]	$[redacted]
SEVERE	Scam	Ownership	1	$[redacted]	$[redacted]	$[redacted]
SEVERE	Sanctions	Counterparty	477870	$[redacted]	$[redacted]	$[redacted]
HIGH	Cybercrime Services	Ownership	9	$[redacted]	$[redacted]	$[redacted]
HIGH	Extortion / Blackmail	Ownership	49	$[redacted]	$[redacted]	[redacted]
HIGH	High-Risk Exchange	Ownership	283251	$[redacted]	$[redacted]	$[redacted]
HIGH	Malware	Ownership	1	$[redacted]	$[redacted]	$[redacted]
HIGH	Ransomware	Ownership	4	$[redacted]	$[redacted]	$[redacted]
HIGH	Violent Extremism	Ownership	3	$[redacted]	$[redacted]	$[redacted]

Image 3. On-chain transactional risk indicators provide data as to how much illicit activity is flowing through an entity

Finally, the regulator could also use transactional and counterparty data to assess the true jurisdictional footprint of the exchange's customer base. For instance the exchange may claim not to permit US customers to onboard. However, an assessment of its counterparty flows may show up numerous transactions with US exchanges, therefore bringing the exchange under the jurisdiction of US regulations.

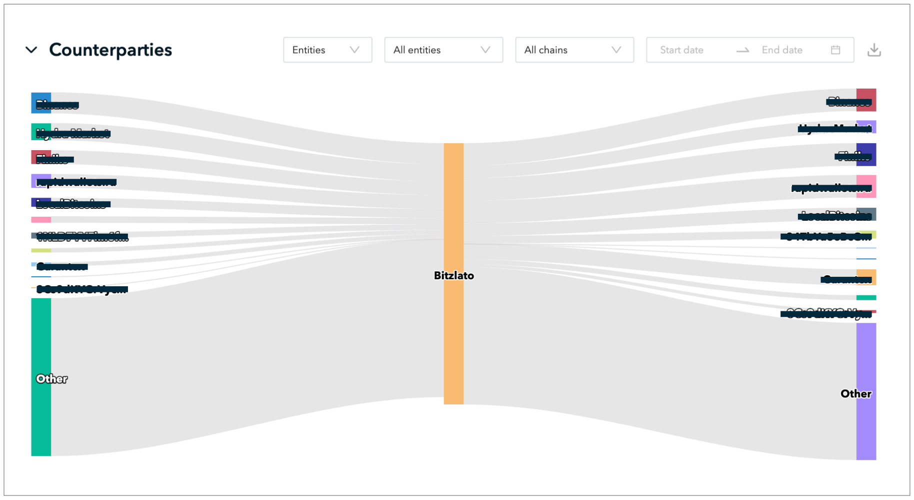


Image 4. Counterparties transaction volume

Such insights could also be applied to an initial regulatory review that signals to examiners where to zoom in and focus resources - a more efficient alternative to blind sampling or reliance on written policies.

And while it is still early, there may be another positive by-product of regulators' use of blockchain intelligence. Historically, it was not uncommon in AML-related enforcement actions for a regulator merely to infer that money laundering or high risk activity took place because of the lack of sound control processes. This focus on process risk by regulators has at times frustrated private sector institutions who posited that process risk did not necessarily equate to financial crime risk.

Today, blockchain intelligence tools can enhance regulators' ability to identify high risk transactions and customers and focus their efforts where actual illicit finance is present, in addition to conducting control evaluations. As the New York Department of Financial Services stated in a recent enforcement action that specifically called out instances of control gaps leading to suspicious activity, the process deficiencies are not "merely theoretical".

Moving from technical compliance to effectiveness

What might real-time supervisory awareness mean for the regulated? It could accelerate another seismic trend that was already taking shape within compliance frameworks – the shift from technical compliance to effectiveness.

Historically, an overreliance on technical compliance risked promoting a check-box approach to compliance. Yet while technical compliance evaluation models assess whether compliance programs satisfy regulations and processes, effectiveness models flip the paradigm and ask questions such as:

- How well does the institution assess, identify and mitigate risks identified in national AML priorities as well as emerging risks?
- Does the output of an AML program provide timely, high-quality and actionable reports to law enforcement?
- When identifying illicit activity, has the institution taken reasonable steps to prevent the risks from happening further? An increase in the number of SARs filed is at times used to assess program effectiveness, but does a decrease in SARs necessarily indicate more *prevention* of illicit activity?

Supranational bodies have already attempted to promulgate a shift to effectiveness models. FATF's landmark report on effectiveness in April of 2022 stated that while the implementation of FATF's 40 recommendations was showing a "significant improvement in technical compliance […] many countries still face substantial challenges in taking effective action commensurate to the risks they face."

An increased focus on effectiveness is also shared by bodies such as the Wolfsberg Group, which has published several guidance pieces on the subject. In 2019, it noted how financial institutions continued to be "examined by national supervisors almost exclusively on the basis of technical compliance rather than focusing on the practical element of whether AML/CTF programmes are really making a difference in the fight against financial crime."

Moreover, recent regulatory feedback on crypto compliance has embraced terms such as "lacks maturity" or the "bare minimum", signaling that effectiveness should be the actual measuring stick.

While both the public and private sector want more effectiveness, challenges abound. One of the primary challenges of moving to an effectiveness model is defining what effectiveness means. How can you evaluate a compliance programs effectiveness?

TABLE OF CONTENTS

Introduction

Designing an effective AML program

Conclusion

Detractors of distributed ledger technology point to the inability of institutions to control illicit finance risks. In fact, the opposite may be true. Blockchain data and analytics tools cannot create effectiveness on their own, but they can provide a clearer snapshot of risk at both the macro (a country's Financial Intelligence Unit) and micro (a customer's wallet address) levels.

This is achievable because at the core of blockchain intelligence is the ability to see and better understand a wide array of different types of risk and determine an institution's vulnerability to those specific risks. As illustrated below, blockchain intelligence allows risk to be broken down by 80+ risk categories like scam, cash to crypto, etc. and by how close that risk is, for example direct risk exposure or a counterparty who customers are transacting with.

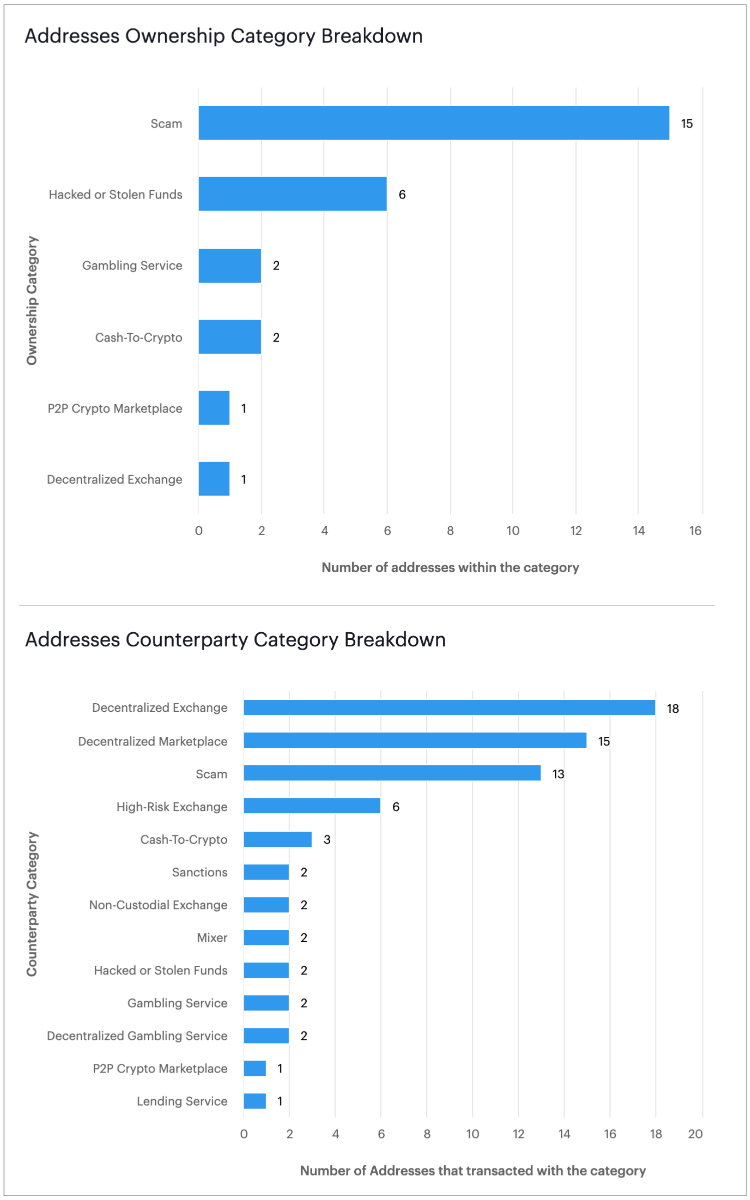


Image 5.
At any given point, institutions are able to understand their risk exposure to illicit activity, irrespective of their alerting configurations

Use Case A

A financial institution (FI) that only conducts fiat business is performing its annual risk assessment. To inform that assessment, the FI will 1) probe subject matter experts as to what they think the most relevant risks are; 2) gather alert and SAR data which may or may not be linked to actual risk; and 3) devise a subjective framework as to what residual risks remain after considering their inherit risks and controls. The output is a mix of qualitative and limited quantitative data that contains varying degrees of speculation and unknown unknowns.

Use Case B

A FI that provides its customers with both traditional fiat banking services as well as the ability to trade and transfer digital assets is kicking off a risk assessment of its digital asset activity. Utilizing blockchain intelligence and irrespective of any controls or surveillance typologies, the FI can answer with granular, quantitative data - 1) the exact risks my customer base is exposed to; 2) which customers specifically have that risk exposure; and 3) how direct or indirect is that risk exposure to the institution.

In contrast to traditional and mainstream AML surveillance typologies, this level of specificity and transparency can help compliance teams better understand which anomalous behavior is likely to be benign and which is actually tied to illicit activity. Identifying and extrapolating risks on-chain can expose the patterns, networks, and facilitators of illicit finance, which can contribute to higher-quality actionable intelligence for law enforcement via SAR reporting. These principles, at the heart of blockchain intelligence, are also the markers of program effectiveness.

Designing an effective AML program

The crypto ecosystem and its risks

Designing an effective AML compliance program that incorporates digital assets or related activities – be it at a financial institution, a crypto exchange, or at the national level – begins with a granular understanding of the digital asset ecosystem. Specificity is key.

Crypto is not monolithic: the digital asset ecosystem is incredibly diverse, with unique differentiation between blockchain types, assets, entities and the activities it conducts. Even the "CeFi"/"DeFi" distinction is insufficiently precise when designing a nuanced and effective compliance program adequately tailored to specific, current risks. Take, for example, the stark differences between Circle's USDC stablecoin built using ERC-20 token standards yet backed 1:1 by cash and short-dated US treasuries, and cryptocurrencies built on UTXO blockchains like bitcoin with no backing. Or, Centralized Financial Applications, whose most commonly known form is a crypto exchange, where retail and institutional investors are able to trade and transact in a variety of cryptocurrencies.

In addition to exchanges, the CeFi ecosystem includes numerous other actors: custodians, OTC trading desks, proprietary traders, liquidity providers, lenders, digital asset issuers, payment processors, crypto ATMs, and more. Each provides different types of products, assets and services, with different sourcing tactics for those assets and business models that have specific expected activity to monitor against.

Based on those services, in combination to their jurisdictional profiles, each may have potential exposure to different high-risk entities or countries. Additionally, there will be varying degrees of regulatory obligations, AML controls, and licensing requirements that may be in a state of flux as countries adopt new regulatory frameworks for varying types of blockchain assets and activities. Lastly, all of the above factors heavily influence the specific risks to monitor, mitigate and control. In short, risk specificity must be matched with control specificity.

Compliance officers intuitively understand that bad actors frequently change tactics, adapt their methods, techniques and operating procedures. Sophisticated bad actors are also aware of control environments and know how to exploit them and jurisdictional weaknesses. As such, any risk matrix

TABLE OF CONTENTS

must combine an understanding of the current risk landscape with a sense of how that landscape evolves and adapts to events, enhancing the risk assessment process to better reflect today and tomorrow's criminal activity.

TRM has compiled a **Digital Asset Ecosystem Matrix** which breaks down a variety of these applications and core risk profiles for easy reference. This matrix can serve as a starting point to begin thinking through the specific risks for each business profile.

Centralized Finance	Key Characteristics	Purpose and Anticipated Activity
Financial Applications (examples)		
Centralized Digital Asset Exchanges (e.g. Binance)	Provide platforms for clients to buy/sell/ hold or transfer digital assets. Mostly holders of money transmitter licenses	Provide on-ramp and off-ramp activities, holds client funds and facilitate transfers to private wallets
Custodians (e.g. Anchorage)	Provide secure storage of digital assets on behalf of their clients	Provide storage of client assets and execute transactions at the direction of the clients
OTC Trading Desks / Brokerage (e.g. Kraken OTC)	Connect buyer and seller for digital asset-related trading	Facilitate large private transactions that can be conducted as principal or agent
Proprietary Traders (e.g. Jump Trading)	Investment firm or vehicle uses their own money instead of seeking commissions from clients' trading	Acting as liquidity provider and trade digital assets using the company's own assets
Investment Funds (e.g. Grayscale)	Digital asset investment funds' primary objectives are to invest in digital assets and raise money from 3rd parties	Invest in both digital asset companies or crypto-assets
Lenders (e.g. BlockFi)	Provide loans denominated in fiat currency or digital assets	Loans are highly collateralized and could involve digital assets in a variety of ways (e.g. collateral, margin payments, principal loan, etc)
Digital Asset Issuer (e.g. Circle)	Launch new tokens that can fund the creation of new blockchain-based services and support the development of new cryptoassets or cryptoassets-powered platforms	Issue new tokens to institutional investors or individual investors, facilitate payment and wallet storage features
Payment Processors (e.g. BitPay)	Enable digital asset payments and receive fiat currency in exchange	Provide payment-processing services to merchants and other business entities, can facilitate wallet address generation
Crypto ATMs	Standalone device or kiosk that allows public to purchase or sell digital assets at a terminal by using cash or debit	Purchase, sell or transfer digital assets for individual use

Centralized Finance	Key Characteristics	Purpose and Anticipated Activity
Non-financial Applications (examples)		
Gaming and gambling (e.g. Axie Infinity)	Video games that incorporate cryptography-based blockchain technology	Online gambling using digital assets as a payment instrument or receiving digital assets as proceeds, game-tokens may be swapped for other assets, play-to-earn proceed generation
Art / Collectables (e.g. OpenSea)	A collectible digital asset that can be tradeable in the digital world	Purchase the NFT art for personal collection or profit-making through reselling
Metaverse (e.g. Decentraland)	The virtual space that integrates the experience on trading a variety of NFTs, including real estate, art, among others and typically traded again in the secondary marketplace	Purchase game character wearables, lands and other items through Metaverse, engage in profit making by purchasing items through Metaverse and reselling
Mining (e.g. Riot Blockchain)	Entities that earn digital assets by verifying transactions on the blockchain on a PoW mechanism	Mining for the miner's own benefits and usage, property owners renting the property for crypto mining at scale, professional crypto mining company operating crypto mining at scale

Decentralized Finance	Key Characteristics	Purpose and Anticipated Activity
Decentralized Exchange (e.g. Uniswap)	Facilitate exchange of digital assets by using smart contracts	Participate in the liquidity pool by putting up their funds and receiving token contributions, automated market making for the swap or transfer of digital assets
Lending Protocol (e.g. Aave, Compound)	"Allow users to deposit collateral in the form of cryptocurrency assets and receive assets, typically dollar-denominated stablecoins, in return"	Act as the lender of the protocol to earn interests higher than what is offered by banks, or act as the borrower of the protocol to borrow digital assets for consumption or arbitrage activities
Derivatives (e.g. Synthetix)	Allow users to create synthetic assets on blockchain platforms that track the value of off-chain / "real-world" assets, as well as other on-chain assets	Purchase and sale of derivatives using digital assets very much like traditional exchange activity
Asset Management (e.g. Lido)	• Assist investors by combining their tokens into pools using smart contracts, often for use on other dapps • These pools capture traditional exposure, synthetic structured tokens, or interest-bearing accounts	Invest digital assets to tokenized pooled portfolio of digital assets. invest digital assets to aggregators, which interact with other lending protocols to identify profitable lending services

Insurance (e.g. Nexus)	Leverage the self-executing smart contracts and eliminate the needs for claims adjusters and even claims themselves	Purchase a variety of cover products and be paid out if the claim is approved by the claim assessment process
DAOs	Organizations or businesses that leverage the blockchain's smart contract technology to make shared decisions on behalf of its members	Fundraising, general governance, including voting, or participation in a social network, sell, purchase or swap of digital assets

Blockchain Tools & Service Providers	Key Characteristics	Purpose and Anticipated Activity
Mixer and Tumbler	Services which co-mingle funds from different users, making it challenging to trace funds to their ultimate source	Conceal the identity of the users and the details of the transactions so deposits and withdrawals are difficult to match
Cross-chain Bridges (e.g. cBridge)	• A type of virtual service that allows users to exchange tokens on one blockchain to another • Both centralized bridge (e.g., Binance Bridge) and decentralized bridge exist	Chain hopping to facilitate compatibility and interopability across different blockchains, potentially used to layer transactions and obfuscate trails
Crypto Swap [e.g. ChangeNOW, Shapeshift]	Allow users to swap cryptoassets for other tokens, either on the same or different blockchains	• Exchange cryptos more quickly and efficiently • Illicit swapping of digital assets to a variety of other digital assets or physical cash to launder money
Key Management and Service Providers (e.g. MetaMask, Ledger)	Entities involved in developing infrastructure services that would manage keys on behalf of users or enable users to manage their own keys	Provide online of offline wallet solutions to safeguard private keys

As threats appear, constrict, evolve and adapt, blockchain intelligence enables the public and private sector to observe, analyze, counteract, report on and potentially seize or prevent those flows as they look for cash out points across financial systems. But only with that granular view of risk can those effective outcomes be achieved.

Case Study

Darknet markets (DNMs) are a common threat vertical captured in many blockchain analytic tools. Hydra was one of the world's largest darknet markets before German law enforcement shut it down in April 2022. Using blockchain intelligence, TRM assessed that the vacuum left by Hydra's takedown resulted in a veritable "Cambrian explosion" in darknet markets. Following Hydra's seizure, twelve new Russian-language marketplaces amassed nearly a quarter more volume in a period of five months than Hydra did in the first five months of the year when it was still live.

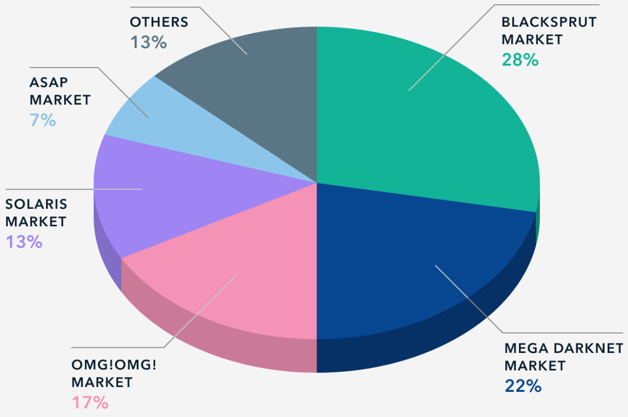


Image 6. Global darknet market share, December 2022.

Emerging risks

Beyond an understanding of the digital assets ecosystem, and the associated risks with each activity and entity type, what are the next steps in designing effective AML programs?

A compliance program's ability to produce valuable and actionable intelligence for high priority risks and targets is one of the best indicators of effectiveness. And to be able to produce those kinds of leads for law enforcement is a better real-time understanding and ability to identify emerging risks within your institution's activity, as opposed to outdated typologies that most criminals have long abandoned.

In 2020, the US Financial Crimes Enforcement Network (FinCEN) released an advance notice of proposed rulemaking on AML program effectiveness that would have called on financial institutions to gather and report information to law enforcement "with a high degree of usefulness to government authorities". Although the legislation has yet to be passed, the advance notice signals the future importance of such information gathering.

Below are several trends growing in scale that compliance officers and regulators can incorporate into their risk assessments to uncover whether they have risk exposure to common tactics used by criminal networks.

Nested exchanges

Nested or "parasite" exchanges do not directly custody clients' digital assets. Instead, they feed off the infrastructure of a large, global cryptocurrency exchange to conduct their transactions. Nested exchanges often take advantage of the greater liquidity and lower transaction costs of big, multinational exchanges while presenting customers with a custom-made interface obscuring the connection to the larger service.

Nested services can present significant risks to the regulated entities whose infrastructure they share. In late 2021, OFAC took what was then the first ever action against a nested crypto exchange called SUEX.io, a concierge cryptocurrency exchanger incorporated in Czechia but operating in Russia. Using its relationship with a large exchange, and access to cash from unknown sources, SUEX was able to convert the illicit monies of its clients to physical cash at an alarming scale.

Todd Conklin, Counselor to the Deputy Secretary of the Treasury, referred to the "illicit underbelly" of nested exchanges, which conduct a disproportionate share of transactions linked to criminality. Nested exchanges continue to be a growing typology, and can at times, be difficult to detect without specialized blockchain intelligence tools. As compliance officers conduct diligence and enhanced due diligence on VASPs, the detection of this typology will be a key indicator speaking to the strength or weakness of AML controls.

As a blockchain intelligence provider that works with some of the world's largest crypto exchanges to help them identify emerging risks such as these, TRM has been studying the on-chain shape and behavior of nested exchanges since early 2020. Today, TRM users leverage this unique capability, known as Ownership Analytics, to identify parasite exchanges and other nested entities operating on their platforms.

Cross-chain criminal activity

Traditionally, bad actors moved proceeds of financial crime through a single blockchain. But in a manner similar to laundering funds through a combination of assets like cash, e-money and securities, criminals are now increasingly chain-hopping to swap cryptocurrencies from one to another as a way of obfuscating the flow of funds.

Over the past year, TRM has seen tremendous growth in the number of bridges being developed to connect blockchains. There are at least 100 bridges connecting blockchains to each other. For web3 and the blockchain ecosystem to grow and thrive, bridges must play a critical part in blockchain interoperability.

The dramatic growth of bridges is important because they allow people to easily transfer value from one chain to another. While this can also be done through exchanges and trading services, those require multi-step processes with significant friction and face well-established AML practices. Bridges, on the other hand, are quick and often pseudo-anonymous because of their architecture. However, bridges have been vulnerable to threat actors.

Bridges are a particular target because they often store large values which help the bridge function. Four bridges were hacked just in 2022 to the tune of over USD 1 billion in crypto (the Ronin Bridge compromise was over USD 600 million, and hackers used bridges extensively to access mixing services on a variety of blockchains).

Cross-chain analytics is especially important because crypto users diversify their crypto assets, utilizing multiple blockchains. As compliance officers upskill their teams to conduct source of funds and source of wealth reviews on-chain, cross-chain analytics will also become an essential tool to detect transfers and understand the provenance of activity across different blockchains.

SQUID scam and laundromat

Exploiting the global frenzy around Squid Game, a violent South Korean drama that became the most watched show on Netflix, scammers launched a tradable token called SQUID. Within weeks of SQUID's launch in October 2021, its price surged by over 40,000%. But when holders rushed to realize their gains, they were locked out by the smart contracts underpinning the tokens. These, it turned out, allowed only the creators to sell. When the creators cashed out, SQUID's price collapsed.

Much more sophisticated than the scam itself was the way its proceeds were laundered. Once the scammers drained liquidity from the pool, they swapped the SQUID tokens several times using a decentralized exchange before sending the lion's share to Tornado Cash. The funds deposited into Tornado Cash were quickly withdrawn and consolidated. The scammers then used bridge applications to move the funds onto the Ethereum network.

Finally, in every scam, one of the biggest challenges for the scammer is how to convert ill-gotten gains into cash. The alleged criminals behind SQUID relied on two crypto exchanges with minimal verification and KYC controls. Analysis by TRM Labs showed that a significant portion of the proceeds was cashed out through an established entity in the crypto ecosystem offering a wide variety of financial services, including the ability to deposit, trade and withdraw virtual assets with no ID checks.

The complicated scheme is a textbook example of the wide variety of tactics and methods used by illicit actors with crypto in a single operation. The collective typologies in the SQUID case in many ways hearken to sophisticated penny stock schemes of the 1990's and 2000's where investors are duped by fraudulent assets or companies and a complex series of steps ensues to sell off the securities across different brokerages, and launder the funds through shell entities and across different points in the financial system with lower controls.

Crypto and NFTs in terrorist financing

Even apparently innocuous blockchain technologies such as NFTs can be used in unconventional ways to further terrorist organization propaganda. The end of August 2022, saw the first instance identified of an ISIS supporter creating an NFT. The purpose of the NFT was likely experimenting with propaganda dissemination, as opposed to raising funds. ISIS itself has not commented on the NFT or on the use of the technology itself.

However, it is important to note that ISIS supporters have long played an important role in trialing new technology and platforms that are later adopted by the group itself. As NFT adoption increases, jihadists will increasingly see it as another medium to spread propaganda and build group identity. Thus, the ability to identify and visualize metadata within a NFT may become increasingly important for compliance officers analyzing these assets and flows that come into contact with them.

Interest in cryptocurrency in general among terrorist groups and their supporters' has grown in 2022, according to TRM's analysis of on-chain transactions, open source information, and proprietary research. While many terrorist financing actors in the space still appear inexperienced, an increasing number are showing growing sophistication and employing various obfuscation techniques, particularly terrorist facilitators operating in Syria and the Gaza strip.

In 2022, terror financing was largely driven by cryptocurrency exchangers that were facilitating terror fundraising campaigns on behalf of individuals and exchanges located in areas controlled by terrorist groups. Another development in the terror financing space is Syria-based cryptocurrency exchanges such as BitcoinTransfer — which is facilitating multiple pro-ISIS fundraising campaigns — have begun experimenting with decentralized exchanges. While the figures remain low, TRM assesses that terror financing through DEX will likely increase as those exchanges' activities on compliant exchanges are disrupted given that they are the subject of a number of law enforcement investigations.

Terror financing actors have changed their cryptocurrency usage in 2022. While Bitcoin has long been the dominant currency, terror financing actors increasingly prefer the use of USDT, with some fundraising campaigns using it exclusively. This trend is likely driven by the price fluctuations associated with BTC as well as the lower fees associated with USDT on TRX.

Terrorist financing has long been difficult for compliance officers to identify. An understanding of the types of assets terrorist financiers may be using, and where those assets may have connectivity to your institution can be leading signals to assist in a compliance officer's review.

Illicit activity facilitation via payment processors

Cryptocurrency payment processors are legitimate services that help individuals and businesses accept cryptocurrency as payment. They generally create payment addresses for customers and provide services that allow users to accept payments directly from their own websites, such as via an API. In return, the payment processor usually receives a small percentage of each transaction.

Unfortunately, the attractive aspects of payment processors that help legitimate entities do business are also attractive to bad actors. Creating new addresses for every payment – or in some cases, reusing addresses for different actors - makes it more difficult for investigators to follow the flow of funds. Without services like payment processors, threat actors would have to manage all payments and addresses themselves. With a payment processor, a bad actor can simply choose one or more forwarding addresses and have everything else managed for a small fee.

Payment processors vary in complexity and compliance controls. They can be as simple and accessible as a Telegram bot. Alternatively, they can be a large functional website that tries to verify its users identity and monitor users for suspicious activity while processing a hundred million dollars' worth of payments per month.

Over the past two years, TRM Labs has seen fraudsters use payment processors as a primary vehicle. This makes sense as they generally want to appear legitimate, like a real business. TRM has identified a large number of investment fraud schemes — some large, some small — that use one of the largest payment processors in the industry.

As compliance teams design risk controls and set risk engine configurations, identifying facilitators of illicit activity flows can be just as crucial as identifying the bad actors themselves.

Key compliance program design principles

The world of crypto can feel overwhelming. There are different blockchain models, UTXO vs. account based chains, permissioned vs. permissionless networks, coin and token types with different backings or creation and burn mechanisms and shifting regulatory obligations. It may at first glance feel daunting when trying to build a first-class compliance program for digital assets that can withstand the coming regulatory scrutiny. And yet, as Churchill said, "out of intense complexities, intense simplicities emerge."

In fact, whether designing an AML program for fiat or digital asset-related activity, the formula for success rests on the same bedrock principles.

Effective AML program design = execution on first principles + risk agility & adaptability + pinpoint targeting

The core principles of effective AML risk management also hold true as the guiding principles behind compliance program design with digital assets. Most of the components of a comprehensive AML program are known:

→

Risk Assessment - the foundation of an effective program, conducted periodically to identify the key risks, controls and vulnerabilities across every business vertical

Blockchain Intelligence Value Add: *Blockchain intelligence (BI) tools have the ability to ingest an institution's transactional activity, and irrespective of how controls are configured, provide a real-time view as to how many risk categories there is exposure to, and how attenuated or not that risk is, providing quantifiable data to feed back into both the risk assessment process and control designs.*

→

Customer Due Diligence - a robust process to identify and verify customer's identity, establish account purpose and expected activity to monitor against and triage higher risk clients for enhanced due diligence (collectively, KYC)

Blockchain Intelligence Value Add: *CDD data typically does not include transactional data points. Yet regulatory expectations are clear that for certain institutions, transactional data can be a meaningful data point to understand the risk of customers. BI tools may be used in the onboarding process or on an ongoing basis to risk score wallet address behavior to enhance and provide a more holistic customer risk ranking that is dynamic and changes whenever the risk exposure changes.*

TABLE OF CONTENTS

Transaction Monitoring/Suspicious Activity Reporting - Written procedures and surveillances in place for timely detection, investigation, escalation and reporting to appropriate authorities

Blockchain Intelligence Value Add: *Traditional TM surveillances key off of transactional properties (size, jurisdiction, velocity, etc.). These have a tendency to produce high rates of false positives as there are many benign reasons why there are changes to a customer's historical activity. BI-based alerts key of actual exposure to specific risks and the behavior of a customer that can be linked to illicit activity.*

Sanctions Screening - Comprehensive process to screen individuals, entities, transactions, IP addresses, etc. on an ongoing basis against relevant lists

Blockchain Intelligence Value Add: *BI tools have the ability to easily incorporate the ability to look for sanctions exposure through TM processes as suggested by OFAC's Virtual Currency Guidance, in addition to viewing sanctions evasion risks that may be downstream from your immediate customer*

Additional Internal Controls - Ensuring the processes work as designed by conducting quality assurance checks, regular audits, independent reviews and surveillance tuning and testing

Employee resources and training - Tools and systems have not replaced the need for experienced, well-trained and informed employees who not only understand the risks but also with the bandwidth to carry out their mandate

Blockchain Intelligence Value Add: *TRM provides a dynamic set of training resources including self-paced certifications, emerging risk overviews, case studies, typologies, threat-actor profiles, and compliance-related upskilling resources*

While these are not novel concepts and have been well-established in the industry for well over a decade, enforcement actions against both traditional and digital asset institutions frequently highlight deficiencies in first principles. Taken over the years, common pitfalls include:

- Stale risk assessments that do not reflect the true inherent risk of the customer base
- KYC programs that gather too little information or lack effective triggers for EDD
- Lack of holistic customer risk profiles that don't take available data into account
- Transaction monitoring (TM) systems configured specifically to decrease alert volumes
- TM processes inadequately staffed leading to large backlogs
- TM processes that flag illicit activity without commensurate SARs or client terminations
- Lack of timely SAR filing

Yet even when best practices are well understood, their successful execution requires a culture of compliance. The recent collapse of FTX shows that an organization can crumble without a culture of compliance within its senior ranks. A top-down approach to risk management has long been a focus for regulators, and will be a rising priority area in the wake of FTX's collapse.

Agility & targeting can help solve for challenges of visibility and scalability

Blockchain data also presents a unique feature not previously available to compliance officers - extended visibility. The ability to see beyond an organization's own books and records can be promising and challenging in equal measure. The transparency of public ledgers enables the ability to ascertain the risk of an entity or one's customer's customers, in order to be more certain about the ultimate source of wealth and funds. But it also raises practical questions.

One of the most common questions asked by compliance officers when first delving into blockchain technology is "how many hops?". How many transactions away from my customer is relevant and regulatorily expected to investigate? The answer depends on facts and circumstances, with more hops not necessarily equating to less risk. Indeed, any prescriptive number would be arbitrary.

TABLE OF CONTENTS

Introduction

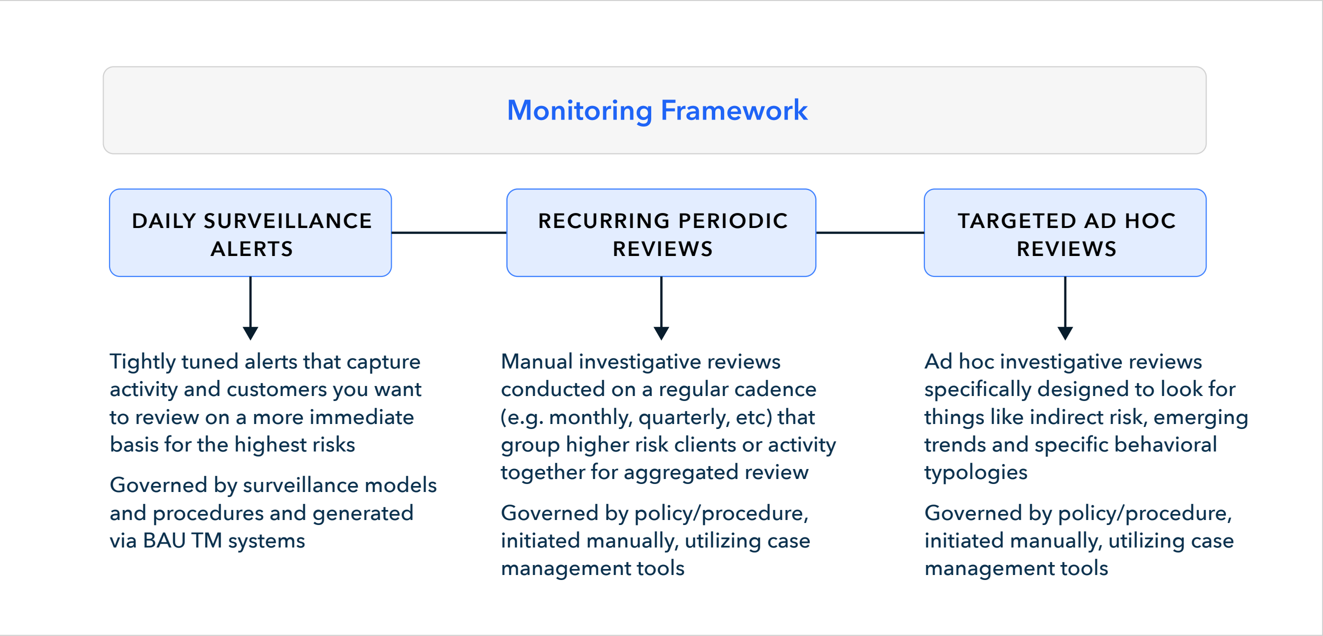
Designing an effective AML program

Additionally, one of the more challenging issues impacting both new and more mature digital asset businesses is how to ensure that a compliance program can appropriately scale when the business and customer base grow exponentially in a short period of time. Scalability was at the heart of the recent enforcement action by the NYDFS against Coinbase.

Within any organization, compliance is acutely affected by rapid changes to a business, and the regulatory expectations to keep pace are high. Regulators frequently cite in enforcement actions this issue of growth-misalignment between business and control-side operations. Moreover, independent of any business growth, larger compliance departments often encounter a variety of challenges that hinder the ability to make quick process changes.

Blockchain intelligence tools are dynamic in both how they can be leveraged and the ways in which a compliance department may zoom in and out to identify risks.

They allow the identification of suspicious activity not to be limited solely to alert driven processes, instead utilizing a broader and more flexible forensic-like approach. The below three-prong framework is one way that can help manage for greater visibility and exponential scaling. Its key principles are a more agile approach to investigative reviews, while also being more targeted to the behavior an investigator is trying to detect.



Monitoring Framework

DAILY SURVEILLANCE ALERTS

Tightly tuned alerts that capture activity and customers you want to review on a more immediate basis for the highest risks

Governed by surveillance models and procedures and generated via BAU TM systems

RECURRING PERIODIC REVIEWS

Manual investigative reviews conducted on a regular cadence (e.g. monthly, quarterly, etc) that group higher risk clients or activity together for aggregated review

Governed by policy/procedure, initiated manually, utilizing case management tools

TARGETED AD HOC REVIEWS

Ad hoc investigative reviews specifically designed to look for things like indirect risk, emerging trends and specific behavioral typologies

Governed by policy/procedure, initiated manually, utilizing case management tools

Through the above framework, an AML department can cover a greater number of higher risk subpopulations in its customer base without a concomitant increase in headcount. For instance:

- Because surveillance alerts have narrow coverage (focusing on the highest risk areas), the output of alerts is lower, leading to fewer instances of backlogs and low quality reviews (i.e. investigators aren't "burning through" alerts)
- That lower volume is balanced out by periodic reviews targeting higher risk customers or activity on a recurring basis, showing regulators the scrutiny those populations receive and enabling a true risk-based approach
- Targeted reviews can be more narrowly tailored to emerging or indirect risks, allowing investigators to go deep and utilize the full transparency of the blockchain

Thus, a partial output of typologies across all three vectors - daily surveillance, recurring periodic reviews and targeted ad hoc reviews - may look something like this:

- Alerts on every instance of customer activity with a darknet market
- Quarterly review on all Politically Exposed Persons (PEPs) and their corresponding on-chain activity
- Monthly review of all high risk customers sending funds to unhosted wallets
- Ad hoc review on all clients where we have filed a SAR and they have indirect risk exposure to high or severe risk category

There can be many variations in how a program looks to execute on principles of greater agility and targeting, but the core elements noted above represent a well-established and effective AML program that regulators now fully expect to see across digital asset businesses.

Conclusion

The market and regulatory events of 2022, followed quickly by the sudden collapse of several established banking institutions, augur the arrival of a higher compliance standard for digital asset businesses. Increased regulatory scrutiny on institutions' ability to demonstrate effectiveness will bring significant challenges to market participants. Blockchain intelligence tools have already become an essential tool to operate in this space.

Such tools are also well-positioned to help demonstrate the strength of AML compliance controls. In the past few years alone, blockchain analytics has grown in leaps and bounds. It now offers extensive coverage of many different blockchains, the ability to trace funds across chains and bridges and flag dozens of different types of risks, as well as emerging behavioral analytics that will be able to identify increasingly complex laundering patterns for investigators. Moreover, developers across the digital asset ecosystem are bringing their own skill sets and technical expertise to build compliance controls directly into network protocols and smart contracts.

Recent regulatory guidance in the U.S. cautioned institutions not to introduce and conduct digital asset activity that can't be mitigated. Armed with the right combination of tools and processes, organizations can ensure that digital-asset-related activities are not only conducted in a safe manner that guards against illicit finance, but also more effectively than the industry has done to date.

TABLE OF CONTENTS

TRM

TRM provides blockchain intelligence tools to help financial institutions, crypto businesses and governments combat cryptocurrency fraud and financial crime.

Find out more:
contact@trmlabs.com
trmlabs.com

BACKED BY AMEX VENTURES BLOCK citi VENTURES PayPal salesforce VISA TIGERGLOBAL Bessemer Venture Partners Y