The Promise and Perils of Crypto:

The Future of Financial Crime Risk in the UAE Crypto Market

THEMIS MENA | ثيميس الشرق الأوسط و شمال افريقيا

Global events over the last year have proven both the immense staying power of the crypto industry while beginning to reveal underlying cracks across such a new and under regulated sector. As the UAE continues to emerge as a key international crypto hub, the potential financial crime risks that accompany crypto activity must be kept front of mind. Whether one works for a virtual asset provider or a financial organisation beginning to deal with crypto, it is important to stay up to date with crypto financial crime risks and compliance requirements in the UAE.

This briefing note serves as a resource for understanding these financial crime risks and regulatory requirements, drawing on UAE and international guidance as well as industry best practices on risk management and enhanced due diligence. It is important for all private sector actors to identify, understand and manage the impact of crypto on their businesses.

Note: The terms virtual assets, digital assets, crypto currency and crypto are used interchangeably in this report – encompassing a digital representation of value that may be digitally traded, transferred, or used as an exchange or payment tool, or for investment purposes. Most regulatory frameworks categorise crypto through virtual assets (VAs) and virtual asset service providers (VASPs).

The UAE Crypto Landscape

The Middle East and North Africa region is the fastest growing crypto market in the world, with the UAE a large contributor to this growth. The country's share in the global crypto market has increased more than 500% since 2020 and its crypto market reached $25 billion in transactional value in 2021. The Dubai Multi Commodities Centre (DMCC) alone has over 500 crypto companies, with the free trade zone focusing on high-impact sectors such as Web3 and blockchain technologies. DMCC also launched a dedicated crypto centre in 2021 to serve as an ecosystem for innovators and entrepreneurs.

With both public and private sector investment in crypto in the UAE, the ability to buy tangible assets using crypto has begun to take shape across the country. Virtual currencies are now accepted by some small UAE-based businesses, such as restaurants and cafes, as a means of conducting transactions. Real estate brokers are also increasingly accepting payment through crypto currencies, as are some airlines.

As more sub-sectors of the economy, including the financial sector, begin to incorporate crypto-related offerings into their existing services, it is critical to take a holistic approach to risk management and consider potential financial crime threats. VASPs and other crypto service providers must also consider their own financial crime risk landscape. Recent events, such as last year's collapse of the crypto exchange FTX, demonstrates the consequences of ineffective governance systems and controls.

Crypto-Related Financial Crime in the UAE

The rise of crypto presents significant vulnerabilities related to financial crime, with criminals found to be engaging in fraud schemes involving crypto currencies or using crypto as a vehicle for money laundering. Globally, crypto based crime surged in 2021 to a reported $14 billion.

The crypto ecosystem creates significant financial crime opportunities by providing a decentralised, pseudoanonymous way to conduct financial dealings. The ability to rapidly transact internationally not only allows criminals to acquire, move, and digitally store assets, often outside the regulated financial system, but also to obfuscate the origin or destination of the funds. Crypto has also spurred the emergence of new business models and activities looking to take advantage of an under-regulated and often misunderstood industry. Such activity presents considerable money laundering, fraud, and market manipulation risks.

There are also increasing risks related to the integration of crypto into mainstream financial service offerings. For example, last year a UAE bank, RAKBANK, announced a partnership with the crypto exchange, Kraken, that will allow Kraken to offer transparent, efficient, dirham-based digital asset trading to their customers. As an institution regulated by the Central Bank of UAE, RAKBANK will enable Kraken, which is licensed by Abu Dhabi Global Market (ADGM), to have their UAE-based clients fund their crypto account through local fund transfers from any bank in the UAE. This risks creating new exposures to financial crime for the regulated financial sector across the UAE, vulnerabilities that might potentially result in new reporting and due diligence requirements to be aware of.

Key Vulnerabilities

The decentralised nature of the sector allows for individuals to send money across borders without the aid of conventional financial systems. No government can have full control over how citizens are using crypto to conduct business or financial dealings. As the financial sector works to integrate crypto more effectively into its anti-financial crime governance and reporting, banks and other financial service providers, such as money transfer services dealing with crypto related transactions, may find themselves facing heightened money laundering and illicit financial flow risks.

Consumers and businesses alike are exposed to fraud schemes using crypto, especially investment scams advertising a get rich quick opportunity. Without proper due diligence and governance, well meaning actors may be left holding the bag with fake or highly volatile virtual currencies.

As VASPs and other crypto businesses set up shop in the UAE, concerns over effective governance and compliance emerge, as the country could find itself dealing with the fallout of any possible criminal activity related to these companies. FTX serves as one such example, as does the infamous OneCoin fraud scheme.

The speed and scale of crypto expansion across the country leaves it more vulnerable to abuse by criminals looking for loopholes in the regulatory environment. The rapidly evolving nature of the regulatory environment also leaves the private sector having to play catch up at times, demanding flexibility from compliance and risk management frameworks.

The crypto sector has also found itself increasingly linked to and involved in geopolitical tensions. Due to the decentralised and global nature of the industry, crypto is increasingly used by illicit actors looking to evade sanctions in their own countries, as well as potentially by governments ostracised from the international system. Iran, for example, has used crypto to pay for imports to circumvent US sanctions against the country. Technological competition across the sector also impacts geopolitical power dynamics more broadly.

Money Laundering

Crypto can be used to circumvent the traditional financial system to launder proceeds of criminal activity, including corruption, fraud, and other crimes such as human trafficking. Increasingly as well, crypto is being embraced by traditional financial services, such as banks, leaving them exposed to illicit financial flows and money laundering.

The International Monetary Fund (IMF) has expressed concern over the use of crypto abused by criminals to transfer proceeds of corruption or circumvent capital controls. According to the Financial Action Task Force (FATF), key forms of crypto related offences relating to money laundering include the sale of controlled substances and other illegal items, fraud, scams, extortion, tax evasion, cyber crimes, child exploitation, human trafficking, sanctions evasion, and terrorist financing. The UAE itself has seen crypto used for money laundering, fraud, and tax and sanction evasion.

- There is growing evidence that organised laundering networks use crypto to layer transactions to hide and transfer illicit assets. Layering can include using multiple crypto wallets, types, and exchange platforms to launder assets numerous times, making it difficult for law enforcement to track their origins.
- Remittance and money transfer services are at higher risk in the UAE for money laundering. Some of these service providers have begun offering blockchain and crypto services, which create additional risks related to anonymity and unregulated financial activity. The expansion of the UAE crypto market into the remittances sector presents a huge risk as the UAE is one of the largest source countries for remittances in the world – with $47 billion remitted in 2020.
- Over-the-counter (OTC) trading desks have started setting up shop in the UAE. OTC desks provide a trading market independent of a regular exchange, letting trades happen directly between two parties (with one of those parties typically being the “desk”). The price setting and transfer of assets occurs between the parties, allowing the transaction to occur outside the public eye.
- Peer-to-peer (P2P) crypto trading platforms are also higher risk, as they can be used by criminals to sell a currency they originally purchased with illicit assets, thereby receiving legitimate money in exchange for criminal proceeds.

It is important to note that while criminals may turn to crypto to launder assets based on a sense of anonymity and privacy, this is a false assumption. The idea that virtual currencies provide full anonymity has been proven incorrect in recent years, with law enforcement in countries such as the US able to trace illicit activity involving crypto back to specific criminals. Blockchain technology is traceable due its transparency element and authorities can look to observe the blockchain and analyse movements and corresponding patterns to identify those that are transacting.

Fraud

Several UAE authorities have raised concerns about crypto asset transactions, including the Abu Dhabi Police warning people to beware of fake cryptocurrency schemes promising instant wealth. Key types of fraud involving crypto include:

- P2P crypto trading platforms don't have a central authority, creating a greater risk of scams. For example, users may create fake profiles or post false information to take advantage of other traders.
- Market manipulation schemes are increasingly commonplace, including pump-and-dump schemes where scammers work together as a group to coordinate price manipulation on a cryptocurrency exchange.
- Giveaway schemes on social media and other online forums are used by fraudsters to trick victims by offering free or discounted virtual currencies in exchange for crypto wallet addresses or other private information.
- Counterfeit or fake currencies are also a key vulnerability for both individuals and businesses alike, where a scammer may sell fake currencies or attempt to use fake currencies at businesses. Fake currencies have made their way onto legitimate crypto platforms, highlighting the difficulty of verification and the importance of due diligence.
- Crypto-romance schemes where the scammer creates fake profiles to snare unsuspecting victims using dating websites and convince victims to invest in fake crypto schemes, are an emerging risk. The Dubai Police have repeatedly issued warnings over this threat in the UAE, such as a recent case where a man lost over a hundred thousand dollars.

There are fairly high levels of appetite for crypto related investment in the country, which risks increasing the level of fraud and other financial crime related to fake investment opportunities. As individuals and organisations look to get involved in the crypto market, criminals may seek to take advantage of their limited knowledge to attract investors for fraudulent schemes. According to a YouGov survey, around two-thirds of UAE residents say they are interested in investing in crypto, with young people the most likely. Moreover, according to a Goldman Sachs survey, around 15% of family offices worldwide have some form of exposure to crypto, with over half considering investing in crypto.

Case Study

One of the most infamous fraudulent crypto currencies globally was OneCoin, which was fraudulently marketed and sold to millions of victims around the world, resulting in billions of dollars in losses. Founded in 2014 by Ruja Ignatova, OneCoin Ltd was registered in Dubai but quickly gained international prominence. For years OneCoin promised big returns and minimal risk, but, as alleged, this business was a pyramid scheme based on smoke and mirrors. Unlike authentic cryptocurrencies, OneCoin had no real value, was not operating on blockchain, and maintained no records of victims' investments.

Ignatova used her reputed magnetic personality to convince individuals with little tech or investment experience to invest considerable sums of money into OneCoin, creating a cult of personality. Claiming to have studied at Oxford and worked at McKinsey & Company (though neither were ever verified), Ignatova gave stadium talks to thousands of people, promising a financial revolution and gaining trust through her expertise and impressive resume. She presented an air of legitimacy and trust, hoping to attract people with narratives of success and money.

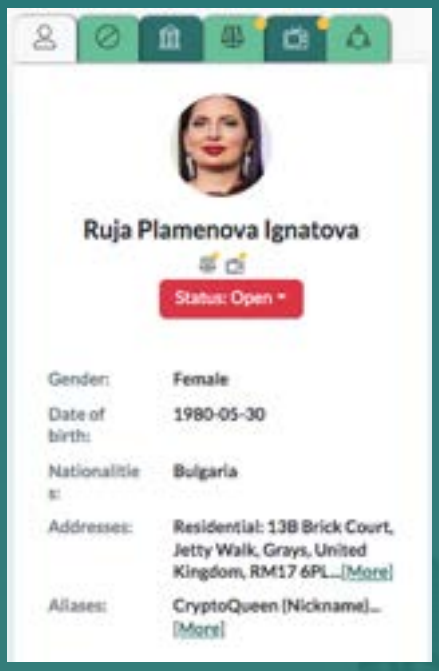
After the fraud was discovered in 2017, Ignatova was indicted by the US – then disappeared, and is now on the US Federal Bureau of Investigation (FBI) Most Wanted List. Potential new details on Ignatova's whereabouts surfaced earlier this year when a property filing to the British government listed Ignatova as the beneficial owner of Abbots House Penthouse Limited, a Guernsey-based company that had purchased a multimillion-dollar penthouse in the London borough of Kensington. Other co-conspirators, including her brother, Konstantin Ignatov, and co-founder, Sebastian Greenwood, have pleaded guilty in the US on related charges. According to the FBI, victims of OneCoin are believed to have been defrauded out of over **$ 4 billion**.

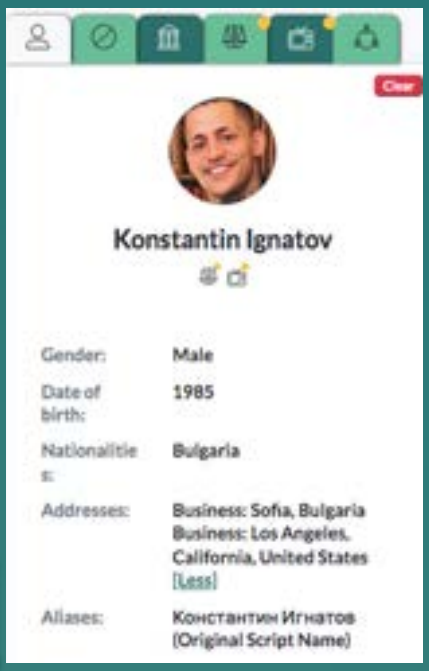
Importance of Enhanced Due Diligence

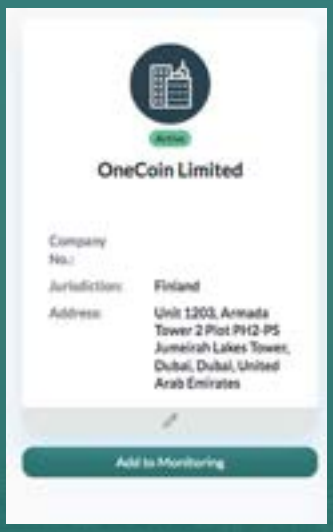
OneCoin investors were left with wiped out savings accounts or thousands of dollars in debt. Before the scheme unravelled, individuals were told to invest quickly in order to get the best deals, enticed by the prospects of large profits. This led to some investors doing minimal due diligence before investing in OneCoin. Others likely felt they didn't need to do due diligence as Igantova claimed an impressive resume with legitimate backing.

This case serves as a clear warning to do your due diligence before investing in or engaging with any crypto related businesses. It is important to scrutinise investment opportunities, recognise the potential for fraud in an under regulated space, and proceed with caution.

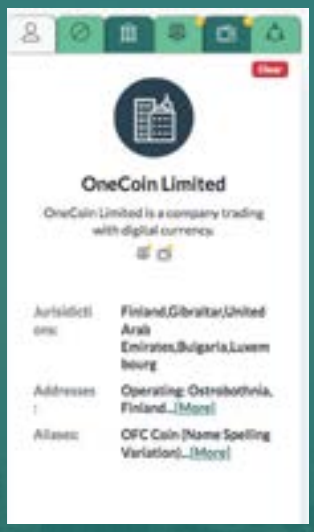
At Themis we provide our clients with smarter due diligence through our tech so it becomes a straightforward, habitual part of everyday working and personal life. Our Search & Monitoring platform allows clients to see the full picture when it comes to financial crime, helping to discover hidden risks and new patterns so our clients and partners can focus on what to do once risks are uncovered. In doing all this, we make it much harder for criminals and organised crime groups to profit from their illicit activity.

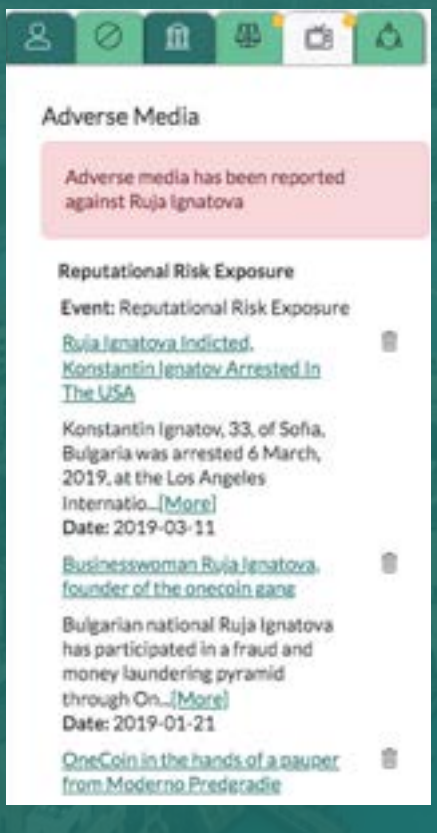

Ruja Plamenova Ignatova
Status: Open
Gender: Female
Date of birth: 1980-05-30
Nationalities: Bulgaria
Addresses: Residential: 13B Brick Court, Jetty Walk, Grays, United Kingdom, RM17 6PL...[More]
Aliases: CryptoQueen (Nickname)...[More]

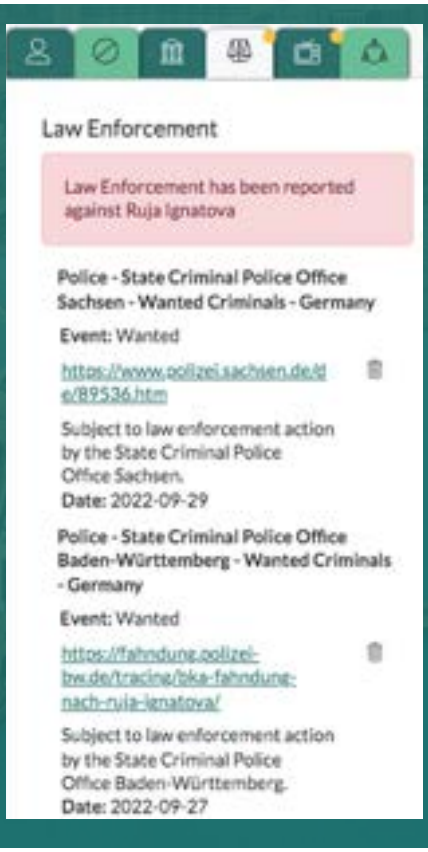

Clear
Konstantin Ignatov
Gender: Male
Date of birth: 1985
Nationalities: Bulgaria
Addresses: Business: Sofia, Bulgaria Business: Los Angeles, California, United States [Less]
Aliases: Константин Игнатов (Original Script Name)

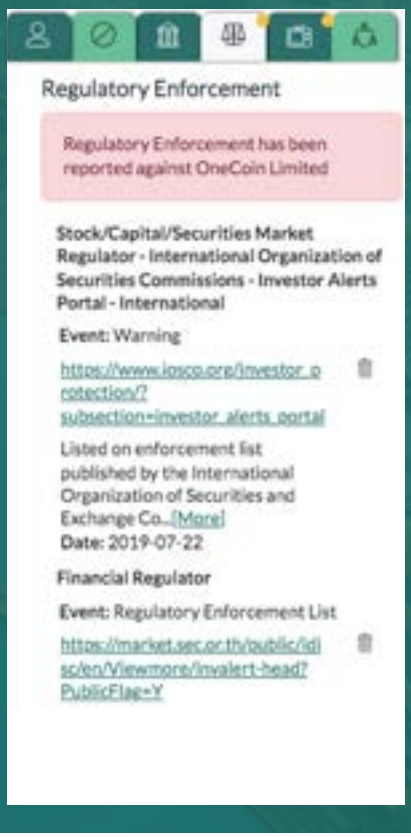

OneCoin Limited
Company No.:
Jurisdiction: Finland
Address: Unit 1203, Armada Tower 2 Plot PH2-P5 Jumeirah Lakes Tower, Dubai, Dubai, United Arab Emirates
Add to Monitoring


One Network Services Ltd.
Pegaron Invest Limited
Martin Breidenbach
OneCoin Limited
Mark S. Scott
Karl Sebastian Greenwood
Ruja Ignatova
Konstantin Ignatov
OneWorld Foundation
OneLife Network Limited


OneCoin Limited
OneCoin Limited is a company trading with digital currency
Jurisdictions: Finland,Gibraltar,United Arab Emirates,Bulgaria,Luxembourg
Addresses: Operating: Ostrobothnia, Finland...[More]
Aliases: OFC Coin (Name Spelling Variation)...[More]


Adverse Media
Adverse media has been reported against Ruja Ignatova
Reputational Risk Exposure
Event: Reputational Risk Exposure
Ruja Ignatova Indicted, Konstantin Ignatov Arrested In The USA
Konstantin Ignatov, 33, of Sofia, Bulgaria was arrested 6 March, 2019, at the Los Angeles Internatio...[More]
Date: 2019-03-11
Businesswoman Ruja Ignatova, founder of the onecoin gang
Bulgarian national Ruja Ignatova has participated in a fraud and money laundering pyramid through On...[More]
Date: 2019-01-21
OneCoin in the hands of a pauper from Moderno Prederadie


Law Enforcement
Law Enforcement has been reported against Ruja Ignatova
Police - State Criminal Police Office Sachsen - Wanted Criminals - Germany
Event: Wanted
https://www.polizei.sachsen.de/de/89536.htm
Subject to law enforcement action by the State Criminal Police Office Sachsen.
Date: 2022-09-29
Police - State Criminal Police Office Baden-Württemberg - Wanted Criminals - Germany
Event: Wanted
https://fahndung.polizei-bw.de/tracing/bka-fahndung-nach-ruja-ignatova/
Subject to law enforcement action by the State Criminal Police Office Baden-Württemberg.
Date: 2022-09-27


Regulatory Enforcement
Regulatory Enforcement has been reported against OneCoin Limited
Stock/Capital/Securities Market Regulator - International Organization of Securities Commissions - Investor Alerts Portal - International
Event: Warning
https://www.ioscp.org/investor_protection/?subsection=investor_alerts_portal
Listed on enforcement list published by the International Organization of Securities and Exchange Co...[More]
Date: 2019-07-22
Financial Regulator
Event: Regulatory Enforcement List
https://market.sec.or.th/public/idisc/en/Viewmore/invalert-head?PublicFlag=Y

Tax and Sanctions Evasion

The use of virtual currency to commit tax fraud and evade taxes is a considerable risk globally. Investors in crypto may be able to shield income from tax authorities, creating an opportunity for wealthy individuals to shift taxable assets into crypto to avoid taxes. Individuals looking to evade taxes in their own countries may turn to crypto exchanges operating in the UAE to attempt to hide assets from tax authorities in their countries.

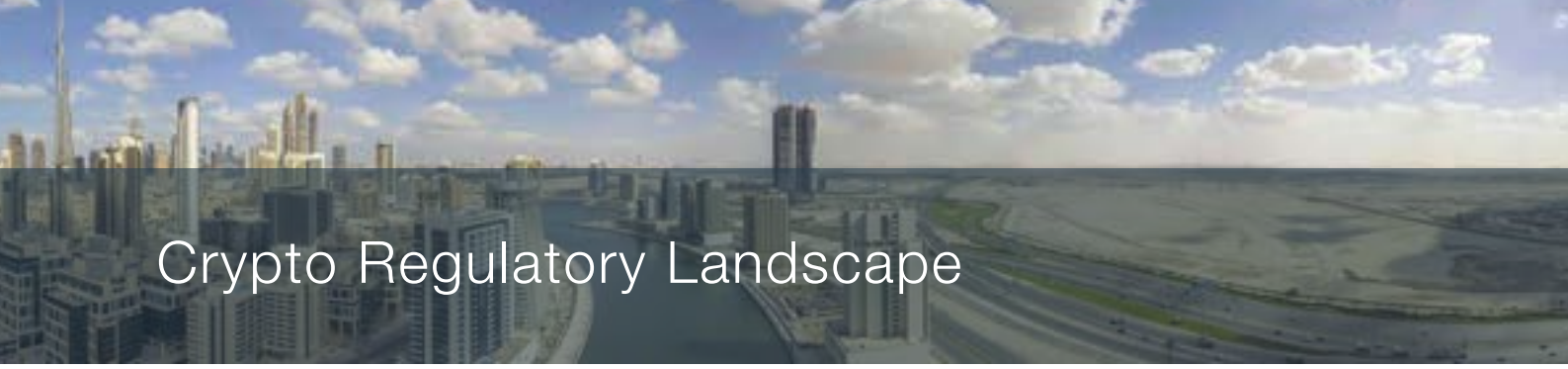
There is also the risk of virtual currencies being used to evade sanctions, highlighted by the US, particularly in the context of Russian entities and individuals. Sanctions / tax evaders and their enablers may attempt to obscure transactions and move money around via virtual currency through the following practices:

- Chain-hopping, the process of crypto users moving rapidly between different currencies, has been used in attempts to move illicit funds or circumvent economic restrictions. For example, North Korean actors have attempted to use chain-hopping to launder stolen crypto currency and evade sanctions controls.
- Mixers and tumbling services are also used by illicit actors. These services combine crypto currencies from various customers, making it harder to determine the source of illicit funds.
- Self-hosted wallets, where the owner has complete control over the wallet, allow for individuals to engage in transactions on a peer-to-peer basis instead of through a third party platform such as an exchange. Self-hosted wallets, by nature, are therefore are not subject to the same regulation as registered VASPs and it is very difficult for law enforcement or other authorities to access the content of the wallet.
- Unhosted wallets, where the wallets are not hosted by an exchange and therefore are not subject to the same regulation as registered VASPs, are a key emerging risk. Unhosted wallets are harder to access and recover without the wallet's private keys, thus also protecting their contents from law enforcement.
- Sanctioned individuals or entities may use proxies such as relatives, shell companies, or stolen identification credentials to access crypto currency and hide assets. Using proxies allows individuals to bypass due diligence and KYC, including potential attempts to block their name and ability to conduct transactions on regulated exchanges and other platforms. In 2020, for example, the US Department of Justice charged a Russian national for using stolen identities to open fraudulent cryptocurrency accounts.

Case Study

Various characteristics of the UAE's real estate sector increase its vulnerability to financial crime abuse, including its high-end nature and internationalised client base. Indeed, the industry was rated by the FATF as facing medium-high money laundering risk; crypto only increases this risk.

There have been reports of Russian buyers attempting to purchase real estate in Dubai using virtual assets, sometimes via intermediaries, who take payment in cryptocurrency and pass cash onto the seller on behalf of the buyer. This presents an emerging challenge for regulators, especially in relation to VASPs. A Reuters investigation has further detailed how crypto firms in the UAE are being deluged with requests to liquidate billions of dollars of virtual currency as targeted Russians seek a safe haven for their fortunes – and as a means to evade US and EU sanctions.



Crypto Regulatory Landscape

As a newer market, global regulation of crypto is evolving rapidly. The sector needs thoughtful regulations to enhance governance and systems across VASPs, financial services, and businesses engaging in crypto to ensure criminal risks are minimised to the fullest extent. International regulators and key jurisdictions, such as the US and the UAE, have begun to consider how existing rules could be applied more effectively and what regulatory gaps remain. However, the level of crypto-related oversight varies greatly from country to country, leaving the industry as a whole grappling with regulatory challenges. In light of this changing landscape, it is important for VASPs and other organisations operating in the crypto space to keep a close eye on new regulatory developments.

International Landscape

The FATF has issued a range of recommendations and regulatory guidance on virtual currencies and other assets. Starting in 2018, the FATF began incorporating virtual currencies into its AML/CFT framework on effective risk management and due diligence. The FATF has since extended its AML/CFT framework to VAs and VASPs, as well as periodically issuing updates and new guidance, most recently in 2022.

- In 2014, the FATF issued Virtual Currencies: Key Definitions and Potential AML/CFT Risks in response to the emergence of virtual currencies and their associated payment mechanisms for providing new methods of transmitting value over the Internet. In 2015, the FATF issued Guidance for a Risk-Based Approach to Virtual Currencies to address the emerging money laundering and terrorist financing risks associated with virtual currency payment products and services.
- In 2018, the FATF adopted changes to its Recommendations to explicitly clarify that they apply to financial activities involving VAs, notably virtual currencies such as crypto, and VASPs. The FATF issued Guidance provides details on how VASPs should be supervised and monitored, including conducting customer due diligence (CDD) and reporting suspicious transactions.
- In September 2020, the FATF also released a report on VA Red Flag Indicators of money laundering and terrorist financing for use by the public and private sectors. See page 14 for more details on red flag indicators.
- In March 2021, the FATF released its Guidance on a Risk-Based Approach to AML/CFT Supervision. While this report addresses AML/CFT supervision broadly, it includes a compendium of information for the AML/CFT supervision of VASPs specifically. In July 2021, the FATF released its Second 12-Month Review of the Revised FATF Standards on VAs and VASPs.
- In 2021, the FATF issued Updated Guidance on a Risk-Based Approach to VA and VASPs. This updated Guidance expands the 2015 VC Guidance document above and further explains the application of the FATF Recommendations for VAs and VASPs. The Guidance also provides private sector entities looking to engage in VA activities with a better understanding of how to effectively comply with the FATF requirements.
- In 2022, the FATF issued an update on its standards on VAs and VASPs. The report updates the FATF's Recommendation 15 and 16 (the FATF Travel Rule), which requires VASPs and other financial institutions to share relevant beneficiary information alongside virtual asset transactions. The report also includes analysis of relevant emerging risks and market developments, such as Decentralised Finance (DeFi) and Non Fungible Tokens (NFTs). It highlights a continued need for many countries to strengthen their understanding of money laundering and terrorist financing risks related to the crypto sector.

- In 2023, the FATF published a targeted update on the implementation of FATF Standards on VA and VASPs that called on all countries to rapidly implement the FATF Standards in regards to VA and VASPs, as it found that jurisdictions continue to struggle with fundamental requirements such as undertaking a risk assessment, enacting legislation to regulate VASPs, and conducting supervisory inspections. The FATF also found that countries have made insufficient progress in implementing the Travel Rule – this lack of implementation creates significant loopholes for criminal to exploit.

In 2022, the OECD published a much-anticipated two-part document — the Crypto-Asset Reporting Framework (CARF) and Amendments to the Common Reporting Standard (CRS) — setting forth a global tax transparency compliance framework with model rules for the automatic reporting and exchange of taxpayer information between countries relating to financial accounts and crypto assets.

- The CRS is a global framework for reporting, obtaining, and automatically exchanging information relating to financial accounts on an annual basis. First developed in 2014, crypto assets and related transactions were not comprehensively covered by the initial CRS. The OECD amended the CRS and developed the stand-alone CARF as a complementary component framework intended to address deficiencies in the original CRS framework.
- The CARF is intended to achieve transparency with respect to crypto asset transactions through the annual, automatic exchange of crypto asset transaction information among the participating jurisdictions whose tax residents hold or engage in crypto transactions. Building on the FATF Recommendations, it covers transactions reporting and due diligence procedures recommendations for organisations.
- CRS amendments look to modernise the framework to cover digital financial products, including focusing on expanding definitions, improving tax due diligence procedures, and designing more detailed reporting obligations.

The OECD also published a crypto-asset reporting framework and 2023 updates to the common reporting standard, which is designed to promote tax transparency with respect to financial accounts held abroad.

In addition to the FATF and OECD, other international regulators and organisations have issued their own guidelines on combating exposure to financial crime across the crypto sector. In 2022, the Basel Committee on Banking Supervision (BCBS) endorsed its global crypto banking rules for implementation by January 2025. These rules include subjecting certain crypto assets to capital requirements based on the risk weights of underlying exposure. The Wolfsberg Group also issued new guidance on Correspondent Banking in 2022, which included recommendations on how to apply its risk-based approach to VASPs.

In May 2023, the international securities watchdog IOSCO unveiled the first global approach to regulating crypto asset and digital markets, drawing on lessons from last year's collapse of FTX and concerns over consumer protection. The proposed standards cover dealing with conflicts of interest, market manipulation, cross-border regulatory cooperation, custody of crypto assets, operational risks, and treatment of retail customers.

Also in May, the EU approved a comprehensive set of rules around crypto, marking the first of its kind. The rules require firms that want to issue, trade and safeguard crypto assets in the EU to obtain a licence. Moreover, the rules outline steps to combat the use of crypto for tax evasion and money laundering.

The UAE Regulatory Landscape

The UAE has sought to balance innovation and economic diversification through crypto with a more cautious regulatory approach to minimise finance crime risks across the industry. Over the past few years, the UAE government has set out concrete regulations on VAs and VASPs, such as guidance issued by the Central Bank (CBUAE) and the Securities and Commodities Authority (SCA).

In terms of AML/CFT legislation, the UAE has its Federal Law No. 20 of 2018 on AML, which defines crimes of money laundering and details federal law applicable across all seven emirates related to regulating the financial and non-financial ("DNFBP") sectors. While it does not mention VAs or VASPs directly, the framework is wide enough in scope it could apply to VAs and currencies.

Under Articles 9 and 15 of the AML-CFT Law, licenced VASPs must report suspicious transactions and information relevant to such transactions to the UAE FIU, and under Articles 13 and 14, supervisory authorities are authorised to assess the risks of VASPs, conduct supervisory operations (including inspections) of VASPs, and impose administrative penalties on VASPs for violations of applicable laws and regulations.

Additionally, the following regulatory developments have taken place in the country in recent years:

- In 2020 the SCA issued regulation concerning Crypto Assets Activities Regulation (CAAR), which regulates the offering, issuing, listing, and trading of crypto assets in the UAE. The regulation covers exchanges, marketplaces, crowdfunding platforms, custodian services, and related financial services based upon or leveraging crypto assets. The CAAR lays down standards and requirements for a wide range of market participants like issuers of securities, investors, trading platforms, and other service providers.
- In 2021 the National Committee for AML/CFT announced the adoption of a regulatory framework for virtual assets in the UAE. The CBUAE and the Securities and Commodities Authority have been tasked with overseeing the implementation of the framework, which will serve as a first step towards a comprehensive regulation of virtual assets.
- In 2022 the Virtual Asset Law No. 4 on the Regulation of Virtual Assets in the Emirate of Dubai entered into force. This law established the Dubai Virtual Assets Regulatory Authority (VARA) to serve as the sole authority regulating all virtual assets (including NFTs) across Dubai's free zones and mainland, except within the jurisdiction of Dubai International Financial Centre (DIFC). VARA is tasked with the regulation and governance of VAs and VASPs on the mainland of Dubai emirate, including facilitating collaborative engagement between global VASPs, industry thought leaders, and international regulatory authorities. Activities subject to authorisation from VARA include operating and managing VA platform services, exchange services, and transfer services.
- In 2023, the Virtual Assets Regulatory Authority (VARA) issued its Virtual Assets and Related Activities Regulations 2023. The regulations set out a comprehensive Virtual Asset Framework built on principles of economic sustainability and cross-border financial security. VASPs that fulfil VARA's licensing requirements will be required to comply with four Compulsory Rulebooks (Company, Compliance & Risk Management, Technology & Information, and Market Conduct). In addition, seven activity-specific Rulebooks have been developed to cater for risks associated with the provision of each Virtual Asset activity (Advisory, Broker-Dealer, Custody, Exchange, Lending & Borrowing, Payments & Remittances, and Management & Investment). VARA has also established rules for the Issuance of all virtual assets, as well as virtual asset marketing activities.
- Also in 2023, The CBUAE issued new AML/CFT guidance for financial institutions when dealing with virtual assets, such as crypto currencies and non-fungible tokens. The new guidance notably covers due diligence for licensed financial institutions when dealing with these customers and counterparties. The guidance, which came into effect in June 2023, applies to banks, finance companies, exchange houses, payment service providers, registered hawala providers and insurance companies, agents and brokers.

Due Diligence and Risk Management Best Practices

As the financial sector continues to embrace crypto, effective due diligence and risk management practices are essential to limit financial crime exposure. It is equally important for VASPs and other crypto related firms to educate themselves on financial crime and train their employees on best practices for due diligence and risk mitigation.

Customer Due Diligence and Monitoring

The new AML/CFT guidance issued by the CBUAE for financial institutions when dealing with virtual assets outlines a risk-based approach to assessing and understanding financial crime risks. For this purpose, LFIs must perform, document, and keep up to date an enterprise-wide risk assessment that includes an assessment of risks related to VASP or VA-exposed customers.

The guidance also outlines customer due diligence measures that Licenced Financial Institutions must conduct before or during the establishment of the business relationship or account.

General CDD measures include:

- Customer identification and verification
- Beneficial owner identification and verification
- Understanding the nature of the customer's business
- Ongoing monitoring
- Sanctions screening

Specific due diligence for all VASP customers include:

- Obtain a copy of the VASPs approval to operate in the UAE
- Understand and assess the VASPs reputation
- Assess the VASP's AML/CFT controls
- Understand and assess the VASPs activity on behalf of third parties

The guidance also outlines enhanced measures for higher-risk customers, as well as requirements for transaction monitoring and suspicious transaction reporting.

The FATF's Recommendation 10 also outlines due diligence measures and describes the scenarios under which financial institutions (FIs) , DNFBPs, and VASPs must undertake CDD measures when engaging in VA transactions. When meeting the outlined thresholds, obligated entities should have in place CDD procedures that they effectively implement and use to identify and verify on a risk basis the identity of a customer, including when establishing business relations with that customer.

Monitoring transactions is an essential component in identifying potentially suspicious activity, including in the context of VA transactions. Transactions that do not fit the behaviour expected from a customer profile, or that deviate from the usual pattern of transactions, may flag suspicions. Monitoring transactions involves identifying changes to the customer profile (e.g. the customer's behaviour, use of products, and the amounts of funds involved) and keeping it up-to-date, which may require the application of enhanced CDD measures.

Red Flag Indicators

The FATF has identified red flag indicators associated with VAs to assist entities, including FIs, DNFBPs, and VASPs in implementing effective anti-financial crime governance and undertaking comprehensive due diligence. The CBUAE references these red flags in its new AML/CFT guidance, highlighting that AML/CFT compliance personnel should be aware of higher-risk transaction patterns and other risk indicators, which may necessitate enhanced due diligence.

Key red flags relating to the size and frequency of transactions include:

- Structuring VA transactions in small amounts to keep them under record-keeping or reporting thresholds, similar to structuring cash transactions.
- Making multiple high-value transactions in a short succession or a regular pattern, activity that is commonly associated with ransomware-related cases.
- Transferring VAs immediately to multiple VASPs, especially VASPs registered in another jurisdiction where AML/CFT regulation is weak.

Key red flags concerning new users' transactions include:

- A new user attempts a large initial deposit to start a relationship with a VASP but the deposit amount is inconsistent with the customer profile.
- A new user attempts to trade the entire balance of VAs or withdraws the VAs and attempts to send the entire balance off the platform.

Other key red flags include:

- Transactions involving the use of multiple VAs, or multiple accounts, with no logical business explanation.
- Making frequent transfers in a certain period of time by more than one person to the same VA account or the same IP address, or concerning large amounts of funds.
- Sender / recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty.
- Discrepancies arise between IP addresses associated with the customer's profile and the IP addresses from which transactions are being initiated.
- A customer's VA address appears on public forums associated with illegal activity.

How Themis Can Help

As financial crime techniques continue to get more complex and present increasing risks to our businesses, we must work harder than ever to ensure we are one step ahead of the criminals and well aligned with regulatory environments. The speed and cross-border nature of the crypto world makes effective due diligence on customers, transactions, and third-parties more difficult. This vulnerability can be overcome with tech-driven solutions that allow for screening and monitoring in real time.

Themis Search & Monitoring can help FIs and others operating across the crypto space uncover client or business stakeholder links to financial crime. The platform offers automated risk mapping capabilities to build out and conduct full due diligence on all extended networks and associated parties. With a click of a button, we provide the ability to automatically spot and analyse how many degrees of separation there is between you and high risk entities and individuals. This helps provide a fuller risk picture on financial crime exposure.

From screening clients looking to make crypto transactions, to crypto companies offering investment opportunities, it is important to conduct due diligence on all transactions and third parties. Being able to identify individuals who have previous criminal history, are sanctioned, or have network associations that are high risk is important to effectively manage financial crime risk across firms. Whenever a high-risk customer or client is identified, it is important to not only screen but monitor these individuals throughout the transaction lifecycle, and Themis tech lets you do just that.

As governments step up their fight against financial crime threats posed by new technologies and novel forms of value transfer, the use of crypto-related sanctions are on the rise as well. At Themis, we screen across 125 sources worldwide to provide you with the latest information on regulatory activity related to sanctions. Whether you are a VASP taking on a new customer or a bank doing business with a VASP, it is important to screen to ensure an individual or entity is not sanctioned in the jurisdiction in which you operate. We recently produced a Crypto Sanctions FAQs document outlining these requirements in more detail – get in touch with us to find out more.

With an office in the UAE, the Themis team has extensive regional expertise, working with both the public and private sectors in the country to help fight financial crime with cutting edge technology, threat-based research and data. Our suite of solutions help firms stay up to date with compliance requirements and we provide the assistance needed to develop governance frameworks to comply with existing and expected regulations in the UAE.

Get in Touch

If you would like to talk to us about any of the themes or updates covered in this report, please let us know.

Nadia O'Shaughnessy
Head of Insight
nadia.oshaughnessy@themisservices.co.uk

Sandeep Sroa
Head of Business Development & MLRO MENA
sandeep.sroa@themisservices.co.uk

Request a call

About Themis

Themis helps clients identify and manage their specific financial crime risks, through a combination of innovation, insight and intelligence.

Our cutting edge platform helps organisations understand these strategic threats through an ESG and socio-economic lens and protects their customers, staff, suppliers and shareholders from criminal attacks or association. For more information, visit www.wearethemis.com

THEMIS

Connect with us

UK: +44 (0) 20 8064 1724
UAE: +971 (0) 58 526 8765
info@themisservices.co.uk

www.wearethemis.com
www.themismena.com

Certified B Corporation

Best for the World 2022 Governance