PYTHAGORAS

Business with cryptocurrencies

The three biggest compliance risks and how to minimize them

1 MONEY LAUNDERING

especially when converting from and into fiat money

2 TERRORIST FINANCING

for example through crowdfunding

3 CORRUPTION

of politically exposed persons or organizations

CHALLENGE

Risks and regulations for trading and services involving cryptocurrencies

Cryptocurrencies are still quite young. The first and most prominent in the global market – Bitcoin – came onto the scene in 2009. Regulatory requirements for transactions involving such currencies are still at a relatively early stage of development. Their scope, status and content vary far more widely internationally than the country-specific rules for traditional financial markets, which cannot be readily applied to cryptocurrencies due to the latter's unique characteristics.

Virtual currencies rely on distributed ledger technologies like blockchains. Their ability to store data securely in decentralized, globally distributed computer networks forms the basis for Bitcoin, Ether, Cardano and similar currencies. Transfers in these types of private currencies can thus be carried out

almost anonymously, without the need for intermediaries such as banks. This also makes cryptocurrencies interesting for criminals, be it in terms of money laundering, terrorist financing, corruption or evading sanctions.

Some of those cases come to light, such as several revolving around the hacker group Lazarus (also known as Guardians of Peace, GOP), which has been linked to the North Korean government. For example, the group gained access to several banks' book money (specifically USD) by means of cyberattacks, converted the money into cryptocurrencies through multiple trading platforms and using various wallets – and after a number of transfers from platform to platform, converted it back into book money. According to U.S. justice officials, several hundreds of millions of dollars found their way into North Korea's coffers in this way.

But many other cases remain unknown. Crypto-related financial crime poses a major challenge for law enforcement agencies, in particular because crypto transactions typically cross borders and requests for mutual legal assistance go unanswered in some countries. So far, we can therefore only estimate how much of the total volume is attributable to criminal activity. What experts agree on, however, is that the value of criminal transactions is probably increasing from year to year – in line with the development of the total market capitalization of all cryptocurrencies. While the maximum market capitalization in 2020 was 700 billion U.S. dollars, 2021 saw highs of more than 2.5 trillion U.S. dollars at times.

New technologies, products, and related services have the potential to spur financial innovation and efficiency and improve financial inclusion, but they also create new opportunities for criminals and terrorists to launder their proceeds or finance their illicit activities.

Financial Action Task Force (FATF)

Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, October 2021

In parallel to the market capitalization of all cryptocurrencies, regulatory pressure on trading and services with cryptocurrencies is growing worldwide. One of the driving forces behind this is the Financial Action Task Force (FATF). Affiliated with the OECD in Paris, it is the primary international body for combating and preventing money laundering, terrorist financing and proliferation financing. For these purposes, the FATF develops compliance standards such as its "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers." Many current laws and regulations are based on these standards, including the 5th EU Anti-Money Laundering Directive, which was implemented in January 2020 in all member states of the European Union as well as in the United Kingdom.

The directive and its implementation acts (e.g., the revised Anti-Money Laundering Act in the EU or the Ultimate Beneficial Owner (UBO) rules in the U.K.) now also place an obligation on crypto traders and service providers, as well as on companies that accept or use crypto assets as a means of payment, to do their part in combating money laundering and terrorist financing. For example, they have a duty to identify their business partners and verify their identity based on documents, data or information obtained from a credible and independent source. When doing business with companies, they must identify the beneficial owner via the commercial register or the transparency register. Comprehensive risk management is also required. Not only do the obligated parties have to develop procedural guidelines and internal policies to prevent money laundering, they must also provide regular compliance training and conduct background checks on their employees. And it doesn't end there. If mandated by the relevant regulatory authority, they must also appoint an anti-money laundering officer. Moreover, they are required to assess customer, product and transaction risk in their day-to-day business. Customers may be politically exposed and therefore vulnerable to corruption, while transactions may be unusual or complex and thus require documentation. The necessary risk analysis must be documented and continuously reviewed. Any suspicious activity must be reported to the relevant law enforcement, customs and tax authorities.

SOLUTION

Identify and minimize risks early on

Much of the risk management and due diligence required when dealing with cryptocurrencies and related services involves knowing who you are doing business with. Pythagoras' know-your-customer and anti-money laundering solutions will help you meet the relevant regulatory requirements conveniently and reliably – right from the onboarding of new customers.

Pythagoras Partner Screening enables you to systematically screen not only existing, but also new business relationships for risks associated with individuals or organizations, as well as to monitor any identified risks. The system automates regular reconciliation with both internal and external reference data, such as from Refinitiv World-Check and Dow Jones Factiva. The integratable native character screening function also supports non-Latin characters, enabling you to use the solution globally while meeting local requirements. Thanks to our **Pythagoras API**, you can also integrate Pythagoras Partner Screening seamlessly into your own applications (e.g., for an account opening process). Whether used this way or as a standalone application: The implementation time is extremely short.

To identify compliance risks related to money laundering, terrorist financing or corruption with cryptocurrencies, you also need to monitor your transactions, especially when fiat money* is converted to a cryptocurrency or vice versa. Exercise caution if any of the following situations occur:

- **The amount and frequency of the transaction does not match the business purpose**
- **Transactions are unusually frequent or short-term in nature**
- **Transactions to and from countries with slacker monitoring of virtual currencies (geographic risks)**
- **Transactions are incongruent with the specified counterparty (for example, payments made from business accounts to private accounts of younger persons)**
- **Transactions with complex patterns that cannot be readily explained**

In cases like these, **Pythagoras Transaction Monitoring** can help. It is easy and fast to implement, compares transaction data with data from your own accounting system and processes it in accordance with a predefined set of rules. You can define rules, parameters and limits either globally, per segment or per individual customer, depending on the level of detail of your organization's data. Any divergence from normal or plausible transactions is indicated and can be documented. Pythagoras Transaction Monitoring records transactions accurately to 15 decimal places – as required for numerous cryptocurrencies.

* Fiat money refers to a national currency that is not tied to the price of a commodity such as gold or silver. The value of fiat money is largely based on the general public's trust in the issuer of the currency – usually the government or central bank of the country in question.

RESULT

Confidence to make the most of business opportunities

Cryptocurrencies enable innovation and new areas of business in the financial market. They have many advantages in their favor:

- **Lower transaction costs than traditional payment transactions**
- **Faster transfer speeds**
- **Efficiency gains for payment systems**
- **Increasing popularity as an investment alternative**
- **High speculative gains possible**

However, as with traditional banking, a key success factor for all this lies in building a culture of mutual trust – between all market players including governments, businesses and consumers. Regulators seek to build and strengthen this trust through compliance guidelines. To comply with these guidelines, be more confident in your day-to-day business and make the most of business opportunities through cryptocurrencies, you will find solutions like Pythagoras Partner Screening and Pythagoras Transaction Monitoring to be indispensable in the future.

CONTACT US IF YOU WOULD LIKE A DEMONSTRATION

Pythagoras Ltd., Bundesstrasse 7, 6302 Zug, Switzerland
www.pythagoras-solutions.com | info@pythagoras-solutions.ch
+41 41 747 12 90