ripple

# Combating Money Laundering Through Compliance and Crypto

According to estimates from the United Nations, upwards of $2 trillion USD per year or five percent of the global GDP is laundered every year. With famous offenders ranging from a Pacific island nation to a gangster dubbed the "Mob's Accountant", these complex operations are used to reintroduce illegally obtained funds into the mainstream financial system.

Money laundering is part of the broader universe of financial fraud and crimes that are often used to finance terrorist actions or underworld organizations. Regulators, law enforcement and financial institutions from around the world routinely coordinate their actions to stamp out these activities and stem the tide of illicit funds.

## Preventing Financial Crime Through Regulation

Anti-Money Laundering (AML) and counter-financing of terrorist (CTF) regulations are key lynchpins in preventing and detecting financial crime. All regulated financial institutions must comply with their local AML/CTF requirements. For example, the United States requires the appointment of qualified a AML officer, annual training for appropriate institutional stakeholders, risk-based procedures for ongoing due diligence, independent testing of an AML program and the establishment of internal controls designed to limit money laundering and terrorist financing risks.

In the United States, the Department of Treasury's Financial Crimes Enforcement Network (FinCEN) administers the Bank Secrecy Act (BSA). The BSA is an anti-money laundering statute that requires regulated financial institutions and other industries vulnerable to money laundering to implement certain controls to guard against financial crime. This includes filing and reporting certain data about financial transactions possibly indicative of money laundering. In 2021, global regulators issued $2.7 billion in AML fines to more than 80 financial institutions as part of their oversight.

To ensure compliance and avoid these penalties, institutions follow well-known and often rigorous sets of best practices for AML and CTF requirements. For example, Know Your Customer (KYC) processes provide visibility into a financial institution's customers, enable monitoring of transactions to spot unusual activity, reporting of suspicious transactions to government authorities, and screening of all customers and transactions to prevent prohibited parties from accessing the financial system.

Yet, even with these controls in place, it is estimated that 90% of money laundering still goes undetected today. Some portray crypto and blockchain technologies as being a powerful tool to circumvent these controls, and while there are some instances where crypto is misused, the vast majority of crypto transactions are not for illicit purposes. Due to the transparent nature of crypto and blockchain technologies, third-party analytical tools can be used to detect money laundering, terrorist financing and other illicit activity. These tools are used by both private and public sectors to combat financial crime.

## Crypto: Financial Crimefighter

Unlike cash transactions, which instantly disappear, the immutable nature of blockchain transactions means that every transaction is enshrined on a chain forever, providing investigators with a clear trail to identify and track illicit transactions and associated wallets.

Because cryptocurrencies' fund flows are highly traceable, suspicious blockchain transactions can be monitored by following direct and indirect connections made through each transaction and by tracing back potentially illegal sources of cryptocurrency funds.

As a result, the technology is increasingly being deployed to identify behavioral changes more quickly in wallets or transactions, trace reported illicit funds and detect risk patterns across transaction parties.

But, as referenced above, financial crimes are not unique to traditional financial institutions alone. Cryptocurrency itself is susceptible to money laundering. While only 0.15% of all crypto transactions in 2021 were considered illicit, crypto fraud is on the rise.

U.S. Treasury Secretary Janet Yellen captured this duality of a technology susceptible to fraud but also well-equipped to combat it when she warned about an increase of risk from digital markets that could also help fight crime.

To diminish this risk and amp up its crime-fighting powers, there are a number of new or in-process legislative acts like the European Markets in Crypto Assets (MiCA) that will further embed crypto into the mainstream financial system. The Chancellor of the United Kingdom also recently announced that stablecoins would become recognized forms of payment in order to be brought under UK regulation.

## Ripple Anti-Money Laundering Policy

Ripple is committed to doing its part to fight financial crime in the financial services technology solutions we offer our customers. Ripple's regulated subsidiaries that are either licensed and/or registered comply fully and continuously with AML and CTF regulatory requirements in the jurisdictions in which it operates, including the U.S. BSA. Besides AML/CTF regulations, Ripple complies with applicable economic sanctions laws and regulations in the jurisdictions in which it operates. As a U.S.-based company, Ripple does not enter customer, transactional or contractual relationships with parties and countries sanctioned by the Office of Foreign Assets Control (OFAC).

At Ripple, we know and understand the importance of compliance and risk management to preserve a healthy financial system. Our technology solutions are designed to offer greater visibility into and control over financial services, and we adhere to the highest global requirements and standards to ensure the integrity of our systems and operations. In this way, we make it possible for financial institutions using our technology products to meet compliance requirements while enjoying the full benefits of instant, affordable settlement technology.