GLOBAL BANKING & Finance review®

FINANCE

What Does The Future Hold For Anti-Money Laundering Practices?

*By **David Schwartz,** President and CEO of the Financial and International Business Association (FIBA)*

Bio: David Schwartz, is the President and CEO of the Financial and International Business Association (FIBA), a nonprofit trade association that is the leading voice for international banking in the U.S., Latin America and the Caribbean. Prior to joining FIBA in 2012, David was Senior Vice President and Manager of International Compliance Risk Management at Regions Financial Corporation.

FIBA is recognized by the financial services industry, regulators, and law enforcement as a Center for Excellence for its knowledge and expertise in anti-money laundering compliance and its high-level education and training programs.

When it comes to the future of banking, much is said about technology's disruptive role in the face of subjects such as digital currencies, digitalization of services, data management and so on, but not nearly enough about Anti-Money Laundering (AML) practices. The reality is that it doesn't matter if we talk and focus on traditional banks, neobanks, fintechs, or even crypto exchanges, *all* financial players should comply with know-your-customer (KYC) obligations and AML regulations.

Contained in the *Anti-Money Laundering Act (AMLA) of 2020* are many provisions that are and will continue to impact the way banks do business and manage their AML programs. These include, but are not limited to, Section 6308, which impacts corresponding banking by allowing the U.S. to ask foreign banks that maintain correspondent accounts in the U.S. for customers' records in their home country or elsewhere, and Section 6403, which requires FinCEN to create a beneficial ownership registry for all companies formed in the US. And while the financial sector is still awaiting guidelines on how to comply with the provisions of AMLA, many are currently reenvisioning their approach to compliance to implement processes and procedures in anticipation of the new rules, such as implementing innovative technology in the areas of beneficial ownership screening, as well as digital identity verification and transaction monitoring systems that can improve their programs are some of the methods under analysis.

As part of AMLA 2020, financial companies are now required to establish streamlined risk-based programs to combat money laundering and the financing of terrorism. Traditionally those very comprehensive risk assessments were undertaken with a simple EXCEL spreadsheet, however, new automated platforms are surfacing such as RiskRator, LexisNexis and Automated Risk Assessment. This comes at a time when financial institutions are welcoming modern technologies to select, implement, and maintain their transaction monitoring systems (TMS) and to better adhere to regulations.

Our society as we have known it, has forever changed in the nearly two years since the AMLA 2020 was passed through Congress. Key players in the banking and finance industry believe we have not yet begun to see the full impact that the global pandemic has wreaked havoc on — socially, economically and culturally. Just the shift in our traditional working environments to virtual/hybrid has forced industries to re-imagine how business is done. Certainly financial institutions are no exception — they have begun upgrading systems and taking a proactive, technology-forward approach to KYC and AML.

One of the many shifts includes the adoption of automated processes to, as appropriate, permit the filing of suspicious activity reports. This is especially important considering criminals are constantly evolving and looking for new ways to hide and move dirty money. Moreover, wrongdoers are not stalled by the bureaucratic burdens needed to implement resources or having to investigate false positives, therefore they are able to work quicker.

It is here where big data, Artificial Intelligence (AI), and machine learning could certainly prove to be highly beneficial. According to the *United Nations Office on Drugs and Crime (UNODC) the estimated amount of money laundered globally in one year is between 2 – 5% of global GDP, or between 800 billion – 2 trillion in current U.S. dollars. Only a tiny fraction of this is recovered through AML practices as, despite best efforts, current systems are not detecting and reporting on most financial crimes.

However, this does not mean financial institutions are not putting in the effort to correct this. Investments in AML practices and procedures have been growing year over year and according to research from *Markets and Markets, it is expected that by 2025 the AML software market will reach 4.5 billion USD, up from less than 900 million USD in 2017. Despite this projected rise in the AML software market, it is up to us, the key financial players, to work together to better streamline the process of combating global financial crime.

Cryptocurrency risks in AML

Another topic that has gained a lot of traction when it comes to AML is the use of cryptocurrencies and their supposed anonymity. The global pandemic and shifts in the financial services industry have helped cryptocurrencies and digital payments become increasingly mainstream these past two years. It has been wrongly believed that crypto allows for complete anonymity in its usage due to digital currencies not being linked to a name, but to a wallet address. The reality is that blockchain technology *is* traceable as records stored there are available to the public and almost impossible to alter. While you might not get a first and last name, a scramble of digits that are unique to a digital wallet and of which the activity can be traced *are* available.

Profits from the sale of cryptocurrencies are considered Capital Gains and taxed by the IRS and there are several legitimate exchanges that have been regulated for almost a decade. In 2013, FinCEN issued guidance for the application of its regulations to persons administering, exchanging, or using virtual currencies (Guidance FIN-2013-G001). Today with AMLA 2020 in place, the *Bank Secrecy Act* is explicitly required to be applied to crypto, treating its exchanges as money services businesses (MSBs). This means that at least in the U.S. crypto exchanges are subject to the Travel Rule which requires financial institutions to pass certain information, such as name and identity of the ordering party of a transaction, on to the next financial institution. Recently, a group of 18 companies, including Coinbase Global Inc. Gemini Trust Co. and Robinhood Markets Inc. set up a platform to help meet conditions of the U.S. Other BSA regulations require customer due diligence be performed and the preparation of Suspicious Activity Reports (SARs) and Cash Threshold Reports (CTRs) where appropriate.

MSBs allow for anonymous transactions of up to $1,000 USD which means transactions under that threshold could go on undetected and continuously be repeated without regulation or causing suspicion. Given that this regulatory system is only for the U.S., the bigger question then becomes, what happens in countries where transactions are unregulated?

In October 2021, El Salvador became the first country to accept Bitcoin as legal tender and its banking system has access to the U.S. financial system through correspondent banks.

The future of banking no doubt includes cryptocurrencies and as their acceptance continues to grow around the world so do the AML risks related to them and in order to mitigate those risks, AML practices will have to evolve. Banking technology is only in its infancy and only time will tell what the future holds.

As a J.P. Morgan executive recently reflected, “We need a globally consistent regulatory framework. It’s important that we get to a solution as quickly as possible.”