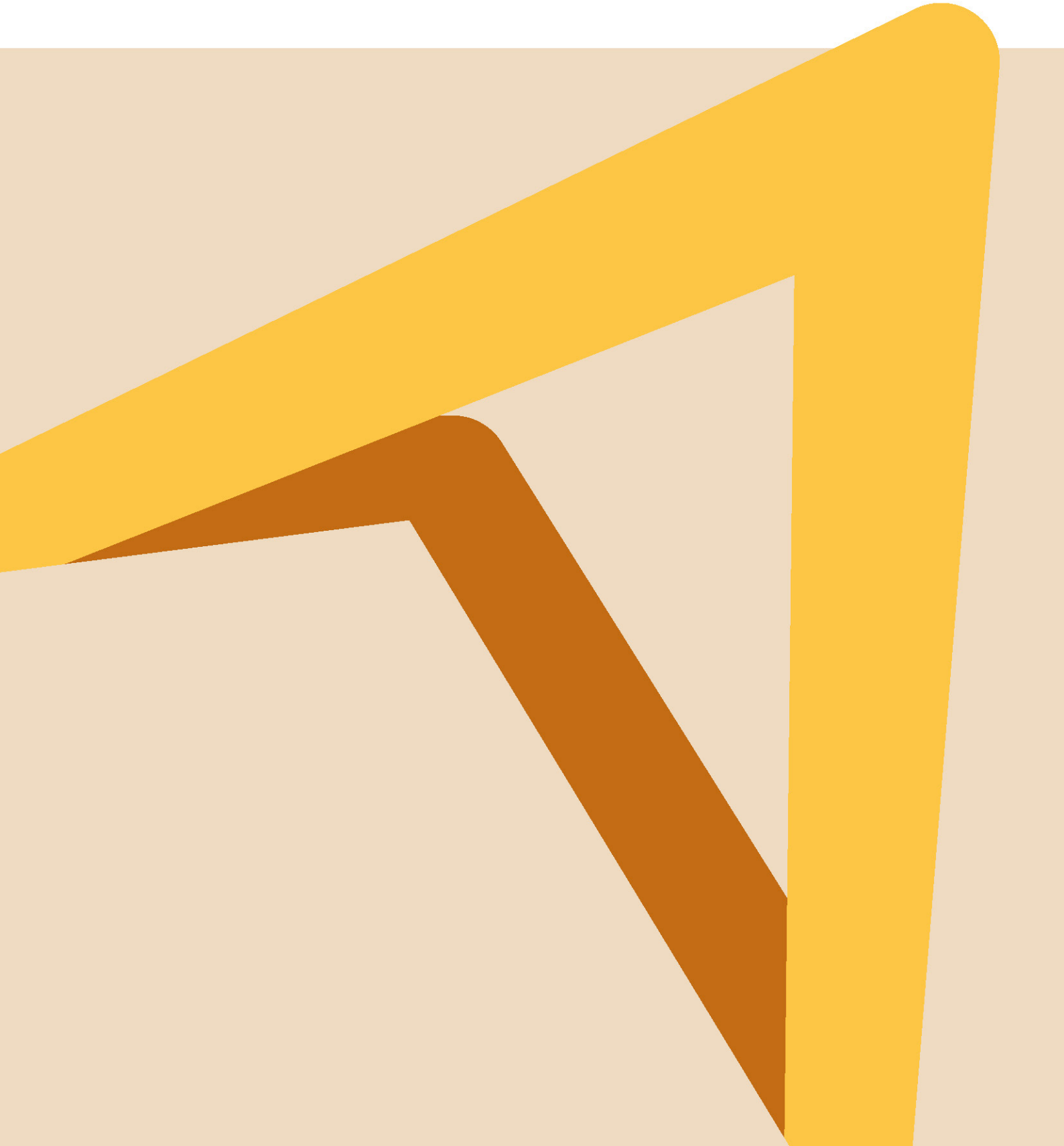
Acuris Risk Intelligence

Thought Leadership

Managing KYC and AML Risks of Cryptocurrencies and Digital Assets



REPRINT

R&C risk & compliance

MANAGING KYC AND AML RISKS OF CRYPTOCURRENCIES AND DIGITAL ASSETS

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JAN-MAR 2019 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine

Acuris Risk Intelligence

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

www.riskandcompliancemagazine.com

ONE-ON-ONE INTERVIEW

MANAGING KYC AND AML RISKS OF CRYPTOCURRENCIES AND DIGITAL ASSETS

Nick Parfitt
Head of Market Planning
Acuris Risk Intelligence
T: +44 (0)20 3741 1200
E: info@acuris.com

Nick Parfitt is responsible for determining Acuris Risk Intelligence's approach to the market and building subject-matter expertise. He has 18 years' experience in project and programme management, business process change and in implementing technology and business solutions at financial services, telecoms and public sector organisations. His experience in the financial crime sector spans seven years, helping tier one financial institutions assess and improve AML, KYC and sanctions operations. Mr Parfitt has worked for several tier one banks in the UK and holds an MBA (Distinction) from Cardiff University, and a BA (Hons) in Biochemistry from Imperial College.

R&C: To what extent would you say cryptocurrencies and digital assets have assimilated into the global financial system? How close are they to becoming mainstream transactions, as far as financial institutions (FIs) are concerned?

Parfitt: It is still very early days for cryptocurrencies and digital assets, and their implications for FIs. The combination of different, early-stage technologies and volatile crypto prices makes it a hard market to predict. Bitcoin is down approximately 80 percent from its 2017 highs, initial coin offerings (ICOs) have been plagued with accusations of fraud and a 2017 EY report found that 30 percent of ICOs have lost almost all of their value. Nonetheless, buoyant ICO markets and investments suggest they are here to stay. Regulators too are increasingly focusing their efforts on the virtual currency space, from an anti-money laundering (AML) and countering of terrorist financing (CTF) perspective. The application of blockchain technology by financial firms to solve specific use-cases shows there is real institutional interest and investment. A recent Morgan Stanley report highlighted that over 17 major global banks are using blockchain to underpin a wide range of use-cases, from escrow management to trade finance, Know Your Customer (KYC), private-label mortgage-backed securitisation (MBS) and derivatives trading.

R&C: How would you describe the risks that FIs face when dealing with digital assets such as cryptocurrencies? How would you gauge the potential for such assets to be exploited by money launderers, for example?

Parfitt: Understanding where the inherent and residual risks are contained within digital assets is key, because different technologies have different levels of anonymity built into their architecture. Monero and Dash, for example, offer far less transparency on the transacting parties compared with Bitcoin. There are also several services which allegedly can offer Bitcoin anonymity through 'washing' or 'tumbling' services, making it hard to know the full provenance of the coin without specialist investigation services and technology. Given the potential for Ponzi schemes, FIs should look at the inherent risks of companies that use ICOs to fund their business models. With approximately 4500 ICOs created to date, the risks are real. Virtual currencies (VCs) will be naturally attractive to money launderers, particularly given jurisdictional arbitrage in AML regulations. Since 2013, FinCEN has treated VC administrators and exchangers as money transmission services and thus subject to standard AML/CTF regulations, notably for both VC-fiat and VC-VC/Alt coins. Europe, on the other hand, has only started regulating through the Fifth Anti-Money

Laundering Directive (5AMLD), and that only applies to VC-fiat conversion.

R&C: Given the increasing use of crypto assets around the globe, what do FIs need to consider with regard to their Know Your Customer (KYC) and anti-money laundering (AML) protocols?

Parfitt: FIs need to understand if they have any exposure to cryptocurrencies throughout their lines of business, as well as their broader business relationships, and whether that is acceptable. Regulations vary widely across the globe and need to be considered in terms of where the FI operates and where its customers do business.

> **"Regulations vary widely across the globe and need to be considered in terms of where the FI operates and where its customers do business."**
>
> *Nick Parfitt, Acuris Risk Intelligence*

R&C: What practical steps should FIs take to strengthen their KYC/AML programmes specifically to address the risks posed by cryptocurrencies?

Parfitt: An enterprise-wide risk assessment will provide insight into an FI's business units, the products and services offered, as well as technology, process and controls, and where the inherent and residual risks lie. At a policy level, the FI's business risk should be clearly articulated. If there is appetite to transact with VCs, currency exchanges, Bitcoin ATM providers or operators and so on, then end-to-end processes and the supporting technology infrastructure need to be assessed to identify and understand the risks and controls. Fundamentally, the business needs to be able to articulate to any of its regulators what it is doing, the reason for the activity and how it is managing any risk exposure. It is no different to introducing a new product or going after a new market. The process of justifying any expansion should be part of an FI's business-as-usual operation, through a well-defined risk management framework.

R&C: What tools are available to assist FIs to manage their KYC/AML programmes and mitigate the risk of money laundering? What do RegTech solutions bring to the table?

Parfitt: There are plenty of tools and rich data sets available to FIs when it comes to understanding and verifying who their customers are, including ultimate beneficial ownership in the case of entities, and the monitoring of transactions or screening for financial crime risk. The use of enhanced due diligence measures for identifying customers' source of wealth or ongoing source of funds is a key area for consideration if significant funds are related to cryptocurrencies. RegTech solutions and niche companies and partnerships can help provide valuable services, such as Bitcoin 'track and trace' forensic tools, as well as creating a community that seeks to educate all participants in financial crime risks and typologies and industry responses.

R&C: With some crypto assets entirely anonymous and unable to be linked to an individual or entity, how can FIs realistically avoid facilitating potentially criminal transactions, even with robust KYC/AML protocols in place?

Parfitt: FIs need to take a risk-based approach to their exposure. This means deciding which crypto assets they will tolerate being exposed to, and ensuring they have adequate controls to monitor their exposure. Privacy coins, such as Monero, will present unique risks to an FI's ability to monitor customer transaction activity, and therefore on their ability to understand the resulting impact on their risk profile. In June 2018, the FCA stated in a letter to firms: "You should take reasonable and proportionate measures to lessen the risk of your firm facilitating financial crimes which are enabled by cryptoassets".

R&C: Looking ahead, what are your predictions for the regulation of crypto assets? How are such regulations likely to impact FIs from a compliance perspective in the long term?

Parfitt: Because they offer the potential for fundamental and beneficial change, virtual currencies will become more widespread and more integrated with the global banking and finance market over time. Regulation today remains uncoordinated and fragmented. Some countries have adopted approaches that are consistent with the Financial Action Task Force's (FATF's) guidance, but many others have not yet done so. However, it is highly likely that regulation will converge globally to form a common standard. The VC industry should look to self-regulate in order to advance an AML/CTF agenda that will complement regulations such as 5AMLD. A key challenge is that the sheer pace of change in this technology leads to regulatory lag. The industry should get ahead of these challenges through public-private partnerships. R&C