LLOYD'S

# Market Bulletin

Ref: Y5196

| | |
|---|---|
| **Title** | Cryptocurrencies, decentralised digitised assets and related transactions |
| **Purpose** | To provide guidance on the writing of insurance products for cryptocurrencies, decentralised digitised assets and related transactions |
| **Type** | Event |
| **From** | Caroline Dunn<br>Head of Class of Business<br>Performance Management |
| **Date** | 6 July 2018 |
| **Deadline** | Immediate |
| **Related links** | |

As cryptocurrencies and other crypto assets are becoming more widespread and acceptable in the commercial world, the insurance market is receiving an increasing number of requests for either specific policies to provide related coverage or amendments to traditional lines in order to provide or clarify coverage. Policies presently available include coverage for private key theft and other hacking and cyber type risks. Lloyd's understands that means of coverage for D&O and Fidelity type risks for businesses such as cryptocurrency exchanges are also being explored, as well as Initial Coin Offering (ICO) related risks.

At present, cryptocurrencies and other crypto assets remain in the early stages of development and acceptance. In some cases the use of cryptocurrencies has also resulted in negative media publicity through their association with criminal activity (for example, in the theft of crypto coins or in their use to support the criminal activity). Regulators and other

financial commentators have also raised concerns about the sustainability of the cryptocurrency and crypto asset market and their values and the legitimacy of ICOs.

In view of their novel nature and the absence of clear regulatory frameworks and precedents for cryptocurrencies and other crypto assets, Lloyd's considers that managing agents should proceed with a level of caution that recognises the risks associated with this class of asset. Where syndicates are to provide coverage in relation to these assets or businesses associated with them, Lloyd's will wish to ensure that managing agents have the required expertise in the underlying risks.

In addition to underwriting considerations, when providing coverage in this class, managing agents also need to have particular regard to the increased risk of financial crime, particularly anti-money laundering and sanctions risks as discussed below. Although not exhaustive, Specie, BBB/Crime, Cyber, PI, D&O and Casualty Treaty are considered among the most exposed lines of business to financial crime risk.

**Lloyd's expectations of managing agents**

- Underwriting considerations

Regardless of whether bespoke policies are created or traditional lines of business are amended to recognise and afford coverage for cryptocurrencies and other crypto assets, syndicates wishing to provide such cover must ensure that they are able to fully evaluate all of the relevant exposures, including consideration of any systemic exposures. These should include considerations relating to matters such as:

- Security of private keys, including ensuring that confidentiality of this information is maintained and whether coverage is provided for "cold" and "hot" storage;
- The integrity of the code standing behind the insured risk and how matters such as subsequent code updates change the risk profile;
- Cyber-crime, hacking risk and underlying network issues that may impact on the insured risk, including technological failure, malicious (or even unintentional) attacks, forks and loss of interest in a particular blockchain leading to failure to maintain the continued processing of transactions;
- The identity of the insured and the scope of coverage in the context of any transaction involving decentralised and/or anonymous actors;
- The insurability of risks and assets in compliance with applicable financial services laws, given the rapidly changing regulatory framework in this area; and
- Exchange rate volatility and exposure to any fluctuations in the value of any underlying crypto asset.

In this regard, a key challenge for insurers is that the underlying technologies for crypto assets are immature and still changing. Managing agents should therefore ensure they understand the implications of developments and changes in such technologies.

Managing agents must also satisfy themselves that policies are compliant with any applicable laws and regulations relating to the insurability of crypto assets at the inception of a policy, during the coverage period, and in the event a policy pays out to an insured.

Policies must only be issued in legal tender (or "fiat currency") with fixed policy limits for the policy term which are unable to be altered by any crypto asset factor, including any exchange rate variation in underlying crypto assets. In respect of a loss, there must be a clearly defined method of valuation clause included in the wording which should include where appropriate an objective mechanism of calculating any relevant exchange rate between fiat currencies and the crypto assets. Payment for coverage should only be made in fiat currency.

Managing agents should note that the following risks must be referred to Lloyd's for prior approval:

- Any products to be offered to consumer customers; and
- Any risks to be written via delegated authority

- Financial Crime considerations

Cryptocurrencies and crypto assets are sometimes associated with supporting criminal activities such as tax evasion, money laundering, contraband (illicit goods) transactions, extortion and circumvention of international financial sanctions. At present, however, cryptocurrencies and crypto assets as well as much of the infrastructure supporting them generally fall outside of current Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF) and Know Your Client (KYC) legislation, both in the UK and in many other countries. Regulators and law enforcement agencies therefore instead have to rely on existing laws and powers to monitor and impose penalties in relation to the criminal use of crypto assets. These powers, however, are often not well suited to the issues that may arise.

The risk for financial crime in transactions involving crypto assets is therefore high and will need to be considered by managing agents when assessing proposals.

The legal and regulatory position is, however, evolving and updated legislation is being introduced in a number of jurisdictions to bring cryptocurrencies and other crypto assets within scope of traditional AML and CTF requirements.

> European Union - the EU's Fifth Money Laundering Directive (5MLD) will bring certain cryptocurrency exchanges and wallet providers within the scope of the AML and CTF controls that already apply to regulated entities. The 5MLD was published in the EU's Official Journal on 19 June 2018 and will enter into force on 9 July 2018. Member States must implement its provisions into national law by 10 January 2020.

United States – On 19 March 2018, in an update to the FAQ section on its website[1], entitled “Questions about Virtual Currency”, the U.S. Treasury’s Office of Foreign Assets Control ("OFAC") advised that it may add digital currency addresses associated with individuals and entities identified to the List of Specially Designated Nationals and Blocked Persons ("SDN List"). All U.S. persons must comply with OFAC regulations, including prohibitions on dealing with parties on the SDN List.

Once OFAC adds digital currency addresses to the SDN List, U.S. persons will be on notice that due to their affiliation with sanctioned parties, transacting payments through those digital addresses will be prohibited. This will mean a greater compliance risk for companies already prohibited from dealing with SDNs. OFAC also advise that its digital currency address listings are not likely to be exhaustive and that if parties identify digital currency information related to an SDN, as well as blocking it, they should notify that information to OFAC.

In view of the additional compliance risks associated with this class, if managing agents decide to provide cover associated with cryptocurrencies and crypto assets or businesses associated with them, which would include associated transactional risks such as ICOs, Lloyd’s expects managing agents to be able to provide appropriate assurances that their own anti-financial crime framework is adequate and proportionate to the risk.

Furthermore, managing agents are expected, where appropriate, to understand and be satisfied that the insured has proportionate anti-financial crime systems and controls in place. This would include ensuring that potential insureds are carrying out effective checks in relation to KYC, AML, source of funds enquiries and, where applicable, OFAC requirements on their own clients and those who may be participating in fundraisings and other transactions.

In addition to the immediate financial crime risks of providing cover to arrangements that may have some association with criminal activity, managing agents need also to have careful regard to the reputational risks to Lloyd’s associated with insuring illegitimate activities associated with these assets. This includes the risk that purchasers of insurance from Lloyd’s may use their association with Lloyd’s to provide legitimacy to an arrangement.

Depending upon the line of business being written, it is important that managing agents obtain and keep on record copies of supporting documentation from insureds, for example:

- Regulatory authorisation(s) and permission(s);
- Policies and procedures;
- Evidence of advice sought from professional advisers;
- Audit reports;
- Banking agreements;
- Outsourced service agreements;

[1] https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs

**Further Information**

If you have any questions regarding Lloyd's requirements for the writing of business in this class, please contact Christian Stanley, Class of Business Manager (Tel: 020 7327 5052; email: christian.stanley@lloyds.com).