LEGAL RISK LLP
SOLICITORS

www.legalrisk.co.uk | 0345 330 6791 | info@legalrisk.co.uk

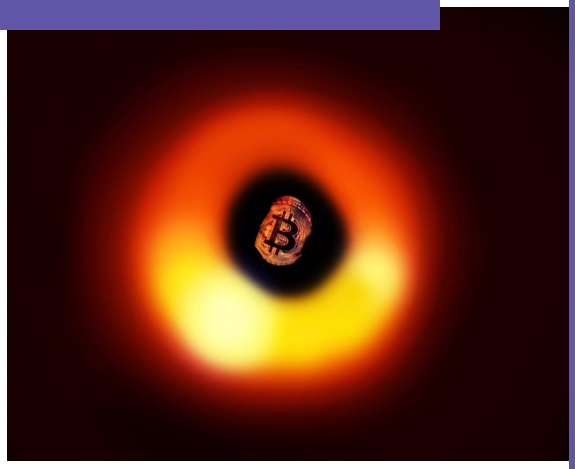
Issue No: 102

Risk Update • November 2021

Cryptoassets - what are the risks for law firms?

Law firms may be wary of the risks of cryptoassets, if only from fear of the unknown. Their insurers may be equally wary – take note.

We have attempted to identify some of the potential risks, but it is early days. It is not open to lawyers simply to decide, to avoid the risk, that cryptoasset issues are not for them: the FCA Perimeter Report 2020/21 stated that 4.4% of UK adults (2.3 million people) own cryptoassets.



Cryptocurrency disappearing into a black hole
Credit: Black hole iStock

For many, their first thoughts will be financial crime and money laundering, terrorist financing from solicitation of charitable donations, and breaching financial sanctions. The risks are there, but cryptocurrency may not in fact be untraceable: the FBI recovered nearly $2.3M of the US$5M ransomware paid following the Colonial Pipeline attack, and the Metropolitan Police recently recovered £180m of bitcoin, after recovering £114m the previous month.

Since January 2020, UK cryptoasset businesses have been subject to The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) and must register with the FCA but 55 are still subject to temporary registration at the time of writing and the FCA has a list of 220 unregistered businesses. Certain specified investments are subject to full regulation within the UK, such as derivatives and units in collective investment schemes, but otherwise cryptoassets are largely outside the scope of FCA regulation. Consequently consumer protection is minimal, which means generally there is no recourse to the Financial Services Compensation Scheme or the Financial Ombudsman Scheme. Many scams have been reported.

For law firms, many of the risks may be similar to those seen in the past, such as failure to identify assets on divorce or in estate administration and volatility in value may cause loss if sale is delayed. In the past we have seen claims from currency losses after acceptance of payment in a currency to which the client had not agreed. Failure to advise a victim of fraud that their property may be recoverable could cause claims given the successes of law enforcement referred to above. However, these examples may be tempered by the FCA's finding that the median holding is only £300.

Investment schemes have caused much financial woe for law firms and insurers, as we have reported several times here, and may be a risk in relation to cryptoassets too. A partner in a major US law firm was convicted of laundering $400m in OneCoin proceeds through a series of private equity funds with bank accounts in the Cayman Islands; prosecutors alleged that $300m was routed through the Bank of Ireland. The introduction of Bitcoin as legal tender in El Salvador may create risk for lawyers wishing to appear cutting-edge by advising on transactions in a country with fairly high financial crime risk. Tax issues will doubtless arise in due course as governments will be concerned not to lose out on revenue.

Other risks from the world of finance which translate to cryptoassets include insider dealing and market manipulation. Much of the business takes place outside the scope of FCA regulation; failing to advise a client that they are dealing with a firm which should be, but is not, regulated could give rise to claims, similar to the unregulated collective investment scheme claims we have seen only too often.

Acceptance of fee payment in cryptocurrency could give rise to own interest conflict issues: in law it is property rather than currency. (A New York City Bar ethics opinion (2019-5) regards it as a business transaction with the client if this method of payment is not optional.) As property, it gives rise to tax considerations – capital taxes, or potentially income tax if traded. Failing to advise clients in some circumstances of the need for record keeping may cause claims as crypto-exchange records may not be available long term.

Reversal of a transaction may be possible in certain circumstances which could expose a firm to liability if they have paid away money

In this Issue

Note

This newsletter is a general guide. It is not a substitute for professional advice which takes account of your specific circumstances and any changes in the law and practice.

Subjects covered change constantly and develop.

No responsibility can be accepted by the firm or the author for any loss occasioned by any person acting or refraining from acting on the basis of this.

following receipt of cryptoassets, in much the same way firms have lost client money by paying out against a cheque which bounced. Hacking of a wallet (including a ransomware attack) could also cause loss.

With a little more crystal ball gazing, there could be liability in some situations for failing to advise clients that use of cryptoassets may imperil their achievement of ESG (environmental, social and governance) targets or contractual obligations: computers that mine bitcoin alone are said to use almost as much power as the Netherlands every year according to the Cambridge Bitcoin Electricity Consumption Index.

Credit: iStock

The commentary on the American Bar Association Model Rule 1.1 (Competence) requires that lawyers there 'keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology…' While that is not set out quite as directly in the UK, poor IT practices have resulted in Solicitors Disciplinary Tribunal fines.

Anti-money laundering (AML)

The Solicitors Regulation Authority (SRA) is expanding its programme of visits to law firms over the next year. These include an in depth examination of the firm's compliance documentation and interviews with fee earners. In some cases this may lead to further regulatory investigations. We have advised many firms on AML compliance since 2003 and on responding to, and achieving a successful conclusion to, investigations.

Several documents have been published since our last edition, and links are on www.legalrisk.co.uk/News. These include –

- Basel AML index 2021 : 10th Public Edition, *Ranking money laundering and terrorist financing risks around the world*
- UK Finance paper, *Making sense of the financial crime risk posed by cryptoassets and how to manage it appropriately*
- Office for Professional Body AML Supervision (OPBAS) *Annual report 2021*
- SRA *First annual report on money laundering pursuant to the Money Laundering and Terrorist Financing (Amendment) Regulations 2019*
- Office of Financial Sanctions Implementation (OFSI) *Annual Review: 2020 to 2021*
- Financial Action Task Force (FATF) *Public Statement on Pandora Papers*
- FATF *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*

Conflicts of interest

The judgment in *Al-Subaihi & Another v Al-Sanea* [2021] EWHC 2609 (Comm) includes an analysis of solicitors' fiduciary duties when negotiating their retainer. (See paragraphs 151 – 160.)

Law Society Practice Note on Conflict of Interests has been updated.

Links to both are on www.legalrisk.co.uk/Conflicts.

Data Protection, Information Security and Cyber Insurance

In *Rolfe & Others* [2021] EWHC 2809 (QB) summary judgment was entered for the defendant solicitors on a claim under GDPR and the Data Protection Act 2018 arising from an email sent to the wrong address. There was no credible case that distress or damage over a de minimis threshold was suffered. A link is on www.legalrisk.co.uk/Data

The Gazette carried a report headed *Emails intercepted in £640,000 conveyancing fraud*. Advice on preventing payment diversion fraud (PDF) has been provided by the National Economic Crime Centre. A link is on www.legalrisk.co.uk/News

The threat of ransomware is a growing concern, evidenced by reports from the insurance market produced by Allianz Global Corporate & Specialty, *Ransomware trends: Risks and Resilience*, and Marsh *UK cyber insurance trends H1 2021*, and the head of GCHQ was reported extensively in the press as saying that the number of attacks on UK businesses has doubled this year. Meanwhile Sophos warned of a phishing scam using Docusign to steal 2FA codes.

Finally, following consultation, the SRA has applied to the Legal Services Board for approval to amendments to the Minimum Terms and Conditions of Insurance to clarify the extent of cover for cyber-related claims.