



Cryptocurrencies and Anti-Money Laundering

The
Strategic
Partner

0203 911 9710

info@thestrategicpartner.co.uk



1. INTRODUCTION

While some law firms have started dealing with digital currency transactions, the rest of the legal sector in the UK predominantly seems wary of cryptocurrency and most legal services providers have yet to be so quick to follow suit.

Some central issues include the potential unethical link between cryptocurrencies and money laundering, the instability of a digital coin's value and the regulator not yet providing a clear position on digital asset transactions.

While digital currency has been around for some time, there are still some major grey areas, both ethical and regulatory, that should be considered. However, if technology continues to advance and more clients request to pay for services by this method, how should law firms react, especially with the current lack of guidance? We highlight some potential risks for firms considering cryptocurrencies as payment methods or dealing with clients with crypto assets as funds and what compliance and risk assessment measures firms must have in place.



2. What is cryptocurrency?

Cryptocurrency is a digital currency (virtual money) that uses blockchain technology to keep track of the currency's worth and ownership — sometimes known as crypto assets, digital coins, or decentralised finance. Some of the most common types of cryptocurrencies include Bitcoin, Litecoin, Ethereum and Ripple. Whilst there are a relatively limited number of banks, credit cards or standard currencies, in comparison, it is thought there are now over 10,000 cryptocurrencies available globally, a figure that seems to be constantly growing.

3. What are the concerns surrounding crypto assets as payment methods?

a) Client identification – One of the primary directives for law firms under [regulation 27 of the Money Laundering, Terrorist Financing and Transfer of Funds \(Information on the Payer\) Regulations 2017 \(MLR 2017\)](#) is customer identification and verification through customer due diligence (CDD) or enhanced due diligence (EDD) in a situation that presents a higher risk of money laundering or terrorist financing. Understanding the source of the client's funds or source of wealth is additionally an integral part of CDD or EDD. This process is relatively straightforward through a bank account and a traditional currency transaction. However, with cryptocurrencies, the process tends to be much more complicated. While many virtual currency and wallet providers already require customers to verify their identities, transactions using cryptocurrencies often allow a degree of anonymity. Individuals and criminal organisations could hide true identities using different aliases and pseudonyms, essentially allowing transactions to be conducted anonymously or to transfer illicit funds without detection. However, moves are in place to strengthen procedures, and updates to regulations should be coming into force in September 2023. The Financial Action Task Force Travel Rule will be implemented in the UK, requiring wallet providers to obtain a lot more information on client accounts as a party depositing into an account. When implemented, it will affect any crypto transactions in the UK over £1,000.



b) Source of funds/wealth – As discussed above, understanding the source of the client's funds or source of wealth is an integral part of CDD and for the purpose of the retainer. One of the directives under regulation 33 provides that you carry out enhanced due diligence and enhanced ongoing monitoring (in addition to client due diligence under regulation 28) where a high risk of money laundering has been identified under your risk assessment or from information provided by a supervisor. Due to the use of crypto assets being identified as a heightened money laundering risk – even without any current guidelines – it seems sensible to assume law firms should be conducting source of funds checks in discharge of client due diligence (CDD) obligations under these circumstances. With cryptocurrency, however, this can prove challenging. Some peer-to-peer platforms enable the trade and acquisition of crypto assets directly between two parties without an intermediary, such as a regulated exchange. There are no CDD requirements as the counterparts directly contact each other. This is obviously cause for concern as it leaves quite a grey area for firms trying to complete appropriate CDD or EDD requirements and their obligation to comply with money-laundering regulations when carrying out source of funds checks.

c) Storing and holding payments – As cryptocurrencies are not 'money' and cannot be stored in a bank, a firm will need to set up a cryptocurrency wallet to accept digital coin payments and handle transactions in this way. Firms are advised to carry out strict due diligence before choosing a wallet provider to ensure that it complies with applicable regulations. For example, **Coinpass** – the British cryptocurrency exchange chosen by some law firms to handle its crypto payments – is registered with the Financial Conduct Authority and has put several measures in place to assist with compliance issues.

d) Professional indemnity insurance – Many professional indemnity insurers are nervous about providing appropriate cover due to the very high risks in this area. So, firms who want to accept payment this way may find it more complicated at renewal period. Firms considering crypto assets as payment must speak with their insurer first or discuss appropriate options at the time of renewal.



4. What are the guidelines from the regulator?

Although the Legal Sector Affinity Group (LSAG) guidance expressly refers to the need for **source of funds checks** under regulation 28 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017), it does not address how to practically approach source of funds checks when crypto assets are concerned. However, a lack of guidance should not be interpreted as an indication that the same regulations do not apply.

In an article from The Law Society on **money-laundering risks associated with digital assets** it is recommended that firms take particular care when dealing with crypto assets and that documented client due diligence and source of funds checks should be carried out, even if the client is not deemed to be high risk as per regulation 35(5) – politically exposed persons (PEPs) for example. It goes on to say that when a firm cannot complete CDD or EDD due to a client being unable or unwilling to provide supporting documents on how specific crypto assets were acquired, the firm may need to cease the relationship in line with regulation 31 MLR 2017.

5. Anti-money laundering compliance – PCPs, training and risk assessments

In our previous article, we highlighted details from the recent **Anti-Money Laundering Annual report 2021-22** and concerns from the Solicitors Regulation Authority (SRA) regarding firmwide risk assessments, AML policies, and controls. The report showed that out of the 224 firms reviewed, more than half – 58% – of the AML policies that were examined needed improving and that a firmwide risk assessment (FWRA) should evaluate the money laundering risks a firm is exposed to.

A fundamental aspect of keeping a firm within a compliant environment is ensuring policies, controls, and procedures (PCPs) fit the firm's operating practices. Crucially, for firms that start dealing with transactions involving cryptocurrencies, any existing PCPs must be reviewed and adapted to ensure they fit the firm's client base and operating style to avoid criticism or scrutiny from the regulator.



Even where a firm decides not to deal with digital currency or crypto assets, notes should be recorded in FWRAs, PCPs and training programmes, with reasons for that decision.

However, PCPs are only as effective as the staff implementing them, so just setting them up is not enough. It is much more about fully understanding and putting responsibilities into practice. The Solicitors Regulations Authority (SRA) has continued to warn firms of its recent findings of failures across the industry and the differences between the firms' PCPs and "what actually happened on the ground". This lack of understanding or failure to put into practice what is contained in a firm's own procedures highlights the crucial part training plays in protecting a law firm and its staff.

Additionally, The Law Society has reinforced the need to move away from 'box ticking' risk assessments and highlighted a firm's obligation to truly understand the clients and matters it is dealing with through a full firmwide risk assessment (FWRA). Firms must go one stage further and document their FWRAs and PCPs, demonstrating they understand their client, the matter they are dealing with and, where necessary, the source of funds and source of wealth.

6. Understanding compliance requirements

Risk management and compliance are required for every law firm, and there is no margin for error. A firm that has not developed a robust approach to managing risk and compliance is in danger of investigations by the regulator, fines, and sanctions, alongside increasing insurance premiums.

Even if your firm is not considering dealing with crypto asset transactions, how confident are you that your AML prevention procedures are adequately maintained and sufficiently applied, and would they hold up to strengthened scrutiny?

Risk and risk management support is central to The Strategic Partner's risk, compliance, and regulation service. Furthermore, our focus is to ensure firms adopt a proportionate and workable solution for case-level risk assessments at the commencement, duration and end of a relationship.



Documenting these assessments is straightforward and requires a process that drives good behaviour into fee earners. This comes as standard in our compliance solutions which provide firms with up-to-date policies, controls, and procedures and a process for risk assessments alongside forms and checklists to evidence the assessment is completed. This is reinforced through training and an independent audit which complies with the requirements of the AML regulations.

If you believe your firm may be at risk or wish to confirm that your firm is achieving the required standard, at The Strategic Partner, we offer a range of solutions.

- **Regulation 21 AML 2017 Independent Audit** – Our service provides firms with a completely independent audit and ensures the review is completed and reported on in accordance with the regulatory requirements. The output will provide the firm with a written gap analysis and solutions to remedy any issues that arise and ensure the firm is compliant, find out more.
- **Training** – Our typical AML training includes:
 - AML training for ALL staff to meet the firm's obligation to provide annual training.
 - One-to-one training for the MLRO and MLCO on their obligations and requirements.
 - Practical training for those involved in client onboarding to ensure ID and AML checks are correctly completed. [Find out more.](#)
- **File Reviews/Auditing** – At TSP we engage with firms undertaking file reviews where we consider procedure, staff, systems, and files to ensure the procedures are up to the required standard and being implemented at case level with a report of the outcome.

We will work with you to ensure your firm operates in a fully compliant environment and stays there. Through achieving this, the compliance officers in the business can be assured and confident that their obligations are being met, enabling them to focus on other areas of the firm.



OUR SERVICES

We will work with you to ensure your firm operates in a fully compliant environment and stays there. Through achieving this, the compliance officers in the business can be assured and confident that their obligations are being met, enabling them to focus on other areas of the firm. Our flagship compliance products are designed to give law firms cost-effective solutions that maintain an ongoing relationship across a 12-month period and beyond. You can view the two packaged services by clicking the following links and viewing our detailed product brochures:

- [Risk, Regulation and Compliance Service including AML](#)
- [Risk, Compliance and AML Guidance and Administration Service](#)

We can also help with:

- [Detailed Firm Strategic Review](#)
- [Risk Assessment and Independent AML Audit Service](#)
- [Process and Document Drafting](#)

For more information about The Strategic Partner or any of our services, you can call us on 02039119710, you can email us info@thestrategicpartner.co.uk or you can visit our website to [make an online enquiry](#).