ALLEN & OVERY

THE DEVELOPING CRYPTOASSET LANDSCAPE IN THE UAE

Spotlight on consumer protection and data privacy

David Berman, Ravinder Mattu and Victoria Ferres

Victoria: Welcome to this Allen & Overy podcast. My name is Victoria Ferres and I'm a senior associate in Allen & Overy's Middle East Financial Services Regulatory group. Here with me is my fellow senior associate David Berman, who is part of our Middle East Litigation, Investigations and contentious Regulatory group ["Hello"]. We are also joined by Ravinder Mattu, a senior associate in Allen & Overy's Middle East Technology and Data Protection team ["Hello"].

This podcast forms part of a series where we will be focusing on key considerations relevant to the emerging cryptoasset landscape in the UAE. This episode will be an overview of the key consumer protection considerations relevant to cryptoassets under the various 'onshore' and 'offshore' legal jurisdictions which make up the UAE. We'll also specifically touch upon data protection regulations which apply to cryptoassets and distributed ledger technology, or DLT, and the key challenges which arise from this.

So David, if I can turn to you first, why is it that consumer protection is such a key consideration when it comes to cryptoassets?

David: It really comes down to the fact that cryptoassets are extremely complex – as we discussed in another of the podcasts within this series, even the term 'cryptoasset' isn't defined, it is purely the umbrella term used to describe virtual assets such as cryptocurrencies, security tokens and so on. Each type of cryptoasset therefore carries its own risks. What this means is that there can be a real lack of understanding on the part of consumers as to what they are purchasing when they buy cryptoassets and what the particular risks are with respect to those assets.

The fact that cryptoassets are constantly evolving at a pretty fast pace is also really relevant.

Victoria: Absolutely. And that means that the nature of the risks posed to consumers is not static. Common risks associated with cryptoassets include those concerned with fraud, misselling and, as you say, the purchase of cryptoassets by individuals who are not fully informed of the complexities of the asset or nature of the market.

As discussed in our episode on the regulation of cryptoassets, whilst cryptocurrencies in particular were originally designed to operate as a unit of exchange, the space has evolved such that the speculative investment of cryptoassets is actually the more common usage: essentially investors investing in the hope that the value of a token will rise against that of fiat currency or other cryptoassets.

David: Exactly and whilst the public may see extreme and sudden increases in the value of tokens as an opportunity to make a return on their investment, the short history of cryptoassets shows us that market crashes are equally severe and there are countless examples of speculators who have lost everything.

Victoria: Correct. Whilst it's true that investors who are experienced in the crypto market will likely recognise both the scale of the pitfalls as well as the potential gains and operate accordingly, less experienced investors will undoubtedly be driven by media headlines around potential gains. These investors, not backed by market experience, and who often won't engage in extensive research and due diligence on the products they buy, are most at risk of suffering significant losses, and are therefore a priority for protection by regulators.

David: Outright fraud has been common as well. Often termed 'rug pulls', numerous scams have been perpetrated by bad actors over the years. By way of illustration, this can involve the generation of a significant amount of hype behind a new token, where the founders promise long-term development and future utilities which encourage investors to buy in. Consequently, the value of the token increases exponentially. Whilst the token's value continues to rise, the developers which made the initial promises will begin to sell their own holdings to make money in the tulip fever-like environment before abandoning the 'project' and leaving those who invested with an asset which essentially has no value.

Victoria: Left unchecked without any form of regulation, investors, particularly inexperienced ones, are left with very few tools to identify which tokens are basically vehicles for scams and those which are bona fide. There are also other risks, not unique to the crypto space, but which regulation can seek to mitigate, such as those concerning data privacy or security of custody of assets.

David: So that's some background as to why consumer protection is so important in the cryptoasset space, but what measures have been introduced in the UAE in order to protect consumers from all these risks?

Victoria: First and foremost having a regulatory framework in place goes some way in itself as a first step to mitigating risks faced by consumers. For example, by requiring tokens to be approved and that persons who provide the means for them to be traded are appropriately licensed.

Crypto businesses that are licensed in the various legal jurisdictions which make up the UAE are required to comply with data protection regulations, for example – that's something that Ravi will discuss a bit later. Regulators will also impose obligations and restrictions on such businesses in relation to the promotion of cryptoassets to the public. This in particular requires that marketing materials are accurate and not misleading, and that they emphasise the speculative nature of crypto and the risks of loss of capital for those which invest in it.

David: Imposing licensing requirements on crypto businesses and obligating them to maintain prescribed professional standards also serves to lend the relevant operators an element of credibility. Examples include regulations requiring licensed businesses to operate in a responsible, honest and professional manner, and to treat customers, and merchants, honestly and fairly at all stages of the business relationship. Being subject to licensing requirements can also mean that licensees have regulatory responsibilities with respect to other third parties in the business supply chain. This essentially requires licensees to do their own due diligence on third parties to ensure they operate in a way which is consistent with UAE laws and regulations, which should make it safer for the consumer at the end of chain.

In theory, consumers should be able to look at tokens supplied in accordance with the regulatory framework as being lower risk, at least as far as threats such as fraud are concerned. Of course, cryptoassets are by their nature high-risk products, notwithstanding the protections supplied by regulation. Where things do go wrong, however, having operators beholden to a regulator can also strengthen the consumer's position in relation to any actions they can take in recourse.

Victoria: And in terms of specifics, we've mentioned before that cryptoassets are regulated differently and by different bodies depending on whether they're offered from mainland UAE or the financial free zones, or even on an Emirate level as we are seeing is starting to happen in Dubai with the recent publication of the Dubai Virtual Assets Law. But let's take a look at the onshore Central Bank regime as an example and particularly the Central Bank's Stored Value Facilities Regulation, or SVF Regulation.

The SVF Regulation prescribes the regulation of digital wallets holding not only fiat currency but also virtual assets. As a licensed stored value facility provider under the SVF Regulation, licensees are required to comply with numerous requirements imposed by the Central Bank with the objective of protecting consumer interests – including, for example, protections around the safeguarding and segregation of customer funds and assets. What the SVF Regulation also does is require licensed persons to comply with the Central Bank's broader Consumer Protection Regulation and Standards which came into force in 2021 and set out extensive consumer protection requirements on all licensed financial institutions.

David: In fact when it comes to SVF providers, consumer protection is so high on the Central Bank's agenda that business conduct and consumer protection is one of seven key areas where prospective licensees are required to obtain an independent assessment of their compliance with the Central Bank's requirements as part of the licensing process.

Victoria: Correct, and consumer protection is similarly high up on the agenda of the other UAE regulators, so it is very much one of the key considerations that both prospective and existing licensees need to be aware of.

Ravi, if I can now turn to you, as we've mentioned, one of the key ways in which principles of consumer protection weave their way into the regulatory regime surrounding cryptoassets and distributed ledger technology is via the implementation of data protection regulations. With that in mind, what are the practical consequences of information on DLTs being subject to these data protection laws?

Ravi: Well, firstly, there's an issue with the logic and terminology of data protection laws, particularly with the concepts of "data subject", "data controller" and "data processor", which seem difficult to apply to blockchains. There is also a lack of clarity as to who is who on the blockchain and what their obligations are according to data protection law.

But the most problematic point of public blockchains with regard to GDPR, and also the DIFC, ADGM and new UAE federal data protection law, is the requirement that the data subject has "the right to be forgotten", meaning that any individual has the right to request that their personal data be erased from the record. Deleting or modifying data on the blockchain is next to impossible, as the data has already been broadcast to all network participants. In addition, a deletion of a record would change the hash of the respective block containing the data and invalidate all the consequent blocks.

Victoria: I can see why that would be an issue. So which of the data protection laws in the UAE specifically refer to cryptoassets?

Ravi: The DIFC data protection law requires companies that perform 'high-risk processing' on a systematic or regular basis to appoint a data protection officer. High-risk processing includes processing that uses new or different technologies or methods that create a materially increased risk to the security or rights of data subjects or render it more difficult for data subjects to exercise their rights. This includes blockchain-based processing of data, which restricts a data subject's right to erasure and rectification. The DIFC data protection law also requires data controllers to inform a data subject about the limitations to request rectification or erasure of their personal data and to ensure the data subject understands and acknowledges the limitation.

Victoria: It's easy to see how DLTs, blockchain and tokens have the potential to revolutionise the way transactions are conducted, but there's certainly a lot of unanswered questions in relation to how data protection laws can be complied with in relation to using crypto-assets so it will be a very interesting area to watch.

That brings us to the end of this episode. As we mentioned at the outset, this does form part of a series of podcasts we are releasing on all things crypto, so do look out for the other episodes. Thanks for listening and please do get in touch if you have any thoughts or comments on this podcast.

David Berman
Senior Associate
Litigation, Investigations and Contentious Regulatory – Middle East
Tel + 971 4 426 7245
david.berman@allenovery.com

Ravinder Mattu
Senior Associate
Technology and Data Protection – Middle East
Tel + 971 2 418 0434
ravinder.mattu@allenovery.com

Victoria Ferres
Senior Associate
Financial Services Regulatory – Middle East
Tel + 971 4 426 7274
victoria.ferres@allenovery.com