Enhanced Protection Against Financial Crimes

Sharif Jamous
s.jamous@tamimi.com
Ahmed Abdulshafe

February 2016

This principle is codified in UAE law by Article 42 of the UAE Federal Law No. 3 of 1987 as amended ("Federal Penal Code"), which states 'Ignorance of the provisions of this law excuses no man.'

The UAE has a relatively young and tech-savvy population, which is extremely active on social media and information technology generally. In addition to its visitors, and peculiarly to the Middle East, the majority of residents in the UAE are from other parts of the world. There is a high turnover of population and movement of people in and out of the UAE, which makes for a diverse and rich environment on a positive note. On the other hand, the world-wide growth in the use of the internet has undoubtedly led to an increase in the number of crimes committed through the use of computers. High disposable incomes and other factors, such as the relative inequality in language abilities, make people in the UAE a target for criminals looking to commit financial crime by electronic means.

This article highlights that the UAE legislature has introduced additional provisions that may be applicable when criminal offences are committed by the use of information technology.

The UAE legislature recognised a need to guard against the misuse of information technology in a law that would protect members of the community and their privacy and send a message to anyone thinking of misusing information technology to commit crime. The result was the promulgation of Federal Law No. 5 of 2012 ("Cyber Crimes Law"), which has now been in force for over three years. Although there have been few convictions under this law so far, given the ongoing rise in the use of technology, there is every reason to believe that the number of investigations and prosecutions will increase as time goes on. In addition to criminalising certain acts that could be described as 'stand alone' information technology offences – such as disabling access to an Information Network or Electronic Site (Article 8) – the Cyber Crimes Law also provides penalties for non-IT offences that are committed by the use of an Information Network, Electronic Information System or Information Technology Tool (Article 37).

Penalties for money laundering

Federal Law No. 4 of 2002 (as amended by Federal Law No. 9 of 2014) ("AML Law") provides the following penalty for acts of money laundering that are committed without the use of information technology:

Article 13:

Whoever commits or attempts to commit an [act of money laundering] shall be punished by imprisonment for a term not exceeding ten years, or by a fine of not less than AED100,000 and not more than AED500,000, or by either of these penalties.

If the perpetrator of a money laundering offence makes use of information technology to commit the crime, however, Article 37 of the Cyber Crimes Law be applicable. This states:

Article 37:

1.Taking into consideration the provisions provided for in the AML Law, any person who intentionally performs any of the following actions using an Information Network, Electronic Information System or any of the Information Technology Tool shall be punished by imprisonment for a period not exceeding seven years and a fine not less than AED500,000 and not exceeding AED2,000,000:

- Transferring, moving or depositing illegal funds for the purpose of concealing or disguising the illegal source.
- Concealing or disguising the reality, source, movement of the illegal funds or the rights related or ownership.
- Earning, acquiring or using illegal funds while being aware that they are from an illegal source.

2. Any person, who establishes, operates or supervises an Electronic Site or publishes information on the Information Network or an Information Technology Tool to facilitate or incite committing any of the actions provided for in Paragraph (1) of this Article shall be punished by the same punishment.

It can be seen that the sentencing provisions that relate specifically to the offence of money laundering in the Cyber Crimes Law are imprisonment up to seven years and/or a fine of between AED500,000 and AED2m. This was an increase in sentencing powers from those available under the AML Law prior to its amendment in 2014. Previously, the sentencing powers available under the AML Law were imprisonment up to seven years and/or a fine of between AED30,000 and AED500,000. Following the amendment in 2014, however, the available sentences under the AML Law are imprisonment up to ten years and/or a fine of between AED100,000 and AED500,000.

Additional penalties under the Cyber Crimes Law

In addition to the sentence available to the court in respect of all offenders, whether UAE nationals or otherwise, the UAE legislator has also included a mandatory requirement to deport foreigners who are convicted of any of the crimes contained in the Cyber Crimes Law. Article 42 states:

Article 42:

The Court shall adjudge to deport the foreigner convicted for committing any of the crimes provided for in this Decree by Law after executing the prescribed punishment.

As Article 42 makes clear, the courts are duty-bound to make a deportation order against a foreign offender. This undoubtedly will send a message as to the seriousness with which such offences are viewed and should be seen as a deterrent, so long as such deportations are reported in the media.

Other ancillary powers available to the court under the Cyber Crimes Law include: confiscating the hardware, software or other items used to commit a cyber crime; closing down premises or websites completely or for a specified period; ordering that the convicted person be kept under close supervision or surveillance, or to deprive him from using any Information Network and Electronic Information System, or to be kept in a therapeutic shelter or rehabilitation centre for the period that the court deems appropriate.

Conclusion

At a time when more and more people are doing more and more online, the presence of a law that combats cyber crimes is potentially just as important as the laws that govern how people behave away

from the world wide web. In accordance with the Cyber Crimes Law, people who use modern technology intentionally to commit crimes will be punished as severely, if not more, than if they had used ‘traditional methods’. Indeed, the Federal National Council is currently considering a draft bill that proposes an increase in the financial penalties available for cyber crimes and re-classifies some offences from misdemeanours to felonies. We will continue to keep an eye on developments in this area and update our readers accordingly.