Oman’s Fight Against Cybercrime and Bank Fraud

- Partner, Head of Office - Oman
- Muscat

Ahmed Al Barwani - Corporate / Mergers and Acquisitions / Commercial
a.albarwani@tamimi.com - Saudi Arabia

Shaima Berri
S.Berri@tamimi.com

Introduction

The Cyber Crime Law issued by Royal Decree No. 12 of 2011 (“**Cybersecurity Law**”) is the relevant legislation in Oman that seeks to address a wide range of illegal activities that are committed through a computer device system or a network. Under the Cybersecurity Law, cybercrimes include intentionally seeking to target networks or computer devices by hacking software or malware, phishing, internet fraud and forgery. Cybercrime is capable of being committed in multiple forms and include sending phishing emails, illegally modifying the data of a computer system with the intention of obtaining an illegal benefit or harming an end user and identity theft.

An important area addressed by the Cybersecurity Law relates to the abuse of personal data and property. The Cyber Security Law makes it a criminal offence to violate personal information and obtain such property through the use of technology. With the advancement of technology and sophisticated methods used to commit cybercrime, the Cybersecurity Law plays an important role in offering protection

to individuals that fall victim to such crimes. A recently reoccurring form of cybercrime has been prominent in the banking sector, in which the banking information of individuals has been illegally obtained to seize and take control over one's financial assets.

This article further expands on the role of cybercrime in the banking sector and how the Cybercrime Law and other regulations are set in place to provide security and protect individuals and entities from such crimes.

The Cybersecurity Law's Role in Banking

The prominence of cybersecurity in the banking sector arises due to the amount of data and information collected and stored by financial sectors. The importance of a bank's confidential data is such that Article 6 of the Cybersecurity Law regards it as a part of the government's confidential data. Banking is a transforming sector and with relatively newer additions and rapid advancement in areas such as digital banking and assets, the sector requires constant adaptation to such changes. Nevertheless, this transformation also leads the way for Cyber-related crimes as banks store sensitive and confidential data.

A recent survey revealed that 58% of the people in Oman were involved in issues relating to financial crimes, which demonstrates that banking is one of the hardest hit sectors by cybercrime. Typically, cybercrime in the banking field occurs as follows: offenders send text messages to victims' telephones posing as their relevant bank branch requesting bank account information on the pretext that their card has been blocked. Once individuals respond by providing such information, the offender proceeds to hack their bank accounts to steal money by transferring lump sums of cash or by conducting a range of online transactions in their favour.

Article 28 of the Cybersecurity Law addresses such issue, making the use of a credit card by those that are not entitled to access such information a punishable offence of imprisonment between one to six months, and imposing a fine between USD 1300 to USD 2600 . The penalty for this crime is also more severe if such person intended to access an individual's bank information and carry out the same activity with full awareness, with a prison sentence between six months to one year in addition to a fine of USD 2600 to USD 13000

Cybersecurity Provided by the Banks

Alongside the internal regulations that banks must strictly follow, the Central Bank of Oman has also required all banks to adapt and comply with the ISO 27001, which is the international standard that provides further specification for the protection of the bank's information security management systems. This system is in place to protect and manage all the bank's information through risk management, with confidentiality and integrity being its central aspects. ISO 27001 also increases organisations' resilience to cyberattack, giving protection to those within the organisation and any external parties such as clients holding bank accounts. An example of such protection would be the installation of preventative software that limits spam emails that could potentially lead to hacking into a bank's information and assets.

Therefore, the ISO 27001, the Cybersecurity Law, regulations from the Central Bank of Oman and the internal regulations and policies imposed by banks conjointly provide a solid framework for financial institutions to fight against cybercrimes.

Awareness and Protection by the Banks

By sending out several warnings through emails and text messages to clients, banks aim to inform all individuals who have bank accounts with them about the ways in which Cybercrime may occur to ensure they do not respond to or believe the fraudulent messages they receive from offenders. Banks have also previously worked with the Royal Oman Police and Information Technology Authority to take further preventative measures by training its staff to battle against Cybercrimes and create further awareness to the public.

Banks use these informative tactics as they would not be responsible to any financial compensation if individuals willingly provide their relevant banking information to such criminals despite having awareness of its consequences. However, banks are also aware that obtaining illegal access to one's banking information can occur in other ways, such as hacking into one's account without making any direct contact with the individual. Therefore, if an individual can prove that they did not willingly give out their banking information to anyone and had their assets stolen because they were hacked, the bank would compensate for any loss incurred as a result of such Cybercrime. The Cybersecurity Law further steps in by penalising the offenders.

Recent and Future Developments in Cybersecurity

Oman has been ranked the third best Arab country and 21st overall in the world in the Cybersecurity Index Report of 2020, released by the International Telecommunication Unit as published in a recent article by Oman Observer. Nonetheless, further developments are underway as alongside the Cybersecurity Law, a Cyber Defence Centre ("**CDC**") has also recently been set up under the Royal Decree No.64 of 2020. The CDC reports to the Internal Security Service, which will issue further bylaws for the CDC to follow to provide stronger protection against cybercrimes. Additionally, the new Draft Law on Cybersecurity and Data Protection may be published in the forthcoming future, which will further regulate cybersecurity and play a significant role in preventing and tackling cybercrimes in Oman.

Conclusion

With the consistent development of technology comes increased dependency on its use, making space for criminals to also depend on digital platforms to conduct crimes. However, such development is also found in the Cybercrime Law. The Cybersecurity Law's implementation into the region tackles this recent wave of cybercrimes, alongside international standards such as ISO 27001 and the relevant regulations adapted by the banks. This framework that banks follow strengthens the cybersecurity measures put in place in Oman and provides additional protection to users from the harm incurred by cybercrimes. Further protection is also ensured with the recent set up of the Cyber Defence Centre in 2020 and upon finalisation of the new Draft Law on Cybersecurity and Data protection.

For further information, please contact Aida Al Jahdhami