Cyber Crimes: Fighting unlawful immitation and fraudulent schemes

Omar Khodeir - Senior Counsel - Litigation
o.khodeir@tamimi.com - Dubai International Financial Centre

September 2015

There is almost always a request for credit card details, or a money transfer, and this money is never seen again.

The Cyber Law No. 5 of 2012 was issued with the aim of protecting individuals (and companies) from cyber crime. It sets out severe penalties for cyber crimes such as fraud, forgery and other fraudulent acts committed using technological platforms. The Cyber Law, with the support of other existing laws, secures the protection of individuals and companies who receive emails from impersonators disclosing false information in an attempt to acquire funds or a benefit.

In this regard, we highlight a recent case handled by Al Tamimi that serves as an example for how these crimes are dealt with.

Facts of the case

The impersonators created a fraudulent website and named it after a well-known investment company based in Abu Dhabi ('the Company'). The Company has an existing genuine website derived from its name and ending with ".com". The fake website changed the company's initials and ended the website with ".org" instead.

Not only did the website state the full names of the Board Members and the CEO of the true Company, it also had several photos of them and gave a background of the Company's business and areas of expertise so that the website would seem as genuine as possible.

The impersonators then contacted individuals and companies to offer investment services. In doing so, they created a fraudulent email with an e-signature referring to the name of one of the Company's senior representatives. They further sent a Non-Disclosure Agreement which had a forged signature of the Company's true senior representative.

One victim transferred an amount of money as a result of receiving the fake email; another discovered the matter at an earlier stage. Fortunately, they contacted the Company through one of its true email addresses which revealed the fraud. In late 2014, the genuine Company attained the domain information for the fake website and the details of the person who had registered it.

Earlier this year, the Company discovered two additional fraudulent websites and the communications that occurred through it, which were almost identical to the previous fraudulent scheme.

Unlawful access and re-publishing information

The above fraud is a breach of the Cyber Law. With certain conditions, the Cyber Law provides for severe penalties for those who enter an electronic site without permission or exceed the limits of the permission to copy, publish or re-publish any data or Information.

The Cyber Law also addresses the circumstance of circumventing the protocol address of the internet by using a fake address or an address belonging to third party or by any other means for the purpose of committing a crime.

Forgery & Electronic Forgery

The existing Federal Criminal Law No. 3 of 1987 details when an act may be considered as a forgery and when anyone committing such an act will be subject to criminal penalties including imprisonment. The Cyber Law tackles specifically any person who has forged and/or who has used an electronic document (with the knowledge of the forgery) and imposes a penalty ranging from imprisonment to a fine.

Fraud

The Criminal Law imposes a penalty of imprisonment or a fine for whoever manages to unlawfully acquire funds using fraudulent acts or by impersonating someone.

The Cyber Law tackles the same concept but mainly for technology platforms. It penalizes a person who unlawfully acquires a benefit by using any fraudulent method or impersonation through an Information Network, Electronic Information System or any of the Information Technology Tools as defined in the Law.

Court orders to close Electronic Sites

Whilst there are a number of potential actions that can be taken against the impersonator(s), the primary aim for the client in this case was to block the fraudulent website so as to prevent harm to its reputation and customers.

The legal strategy was successful in attaining the above outcome. The strategy relied mainly on provisions from the Cyber Law which allows for confiscating the means used to commit any of the crimes provided for in its provisions or by erasing the information along with closing the site where any of these crimes are committed.

By highlighting the massive harm and continuous risks from the breaches committed through accessing the Company’s website to copy and re-publish the information found there; using false email addresses to unlawfully acquire funds; forging a signature; we were able to secure the desired outcome.

The Abu Dhabi Court issued an order to block the fraudulent website on an urgent basis. It was issued in late 2014 and another Court order was issued earlier this year to close the other two fraudulent websites.

Conclusion

The Cyber Law is the main law addressing crimes occurring through the internet and technology platforms. The above case demonstrates the effectiveness of the Cyber Law and the strong action taken by the local courts in implementing it.

However depending on the desired course of action, other laws may be relied on as well. Once there is a discovery of a fraudulent act, early legal assistance is critical to ensure the correct strategy is put in place to prevent the fraudsters and any further harm.